代数学の基礎

佐々木隆二

この本は, 代数学 C,D の講義の詳説と補充, 更に, 代数学の基本的事項全般の解説を意図して書いたものである.

講義の内容をより深く系統的に学習する学生の自習書となるようを,「読みやすく」を心がけて書いたつもりである。

講義中に随時、演習問題とその解答を, 補う予定である.

末尾に、本書を執筆するに際し, 参考にした文献や, 本書で取り扱わなかった代数学の基礎を補うに恰好な文献を列記する.

目 次

第1章　群

1.1　群の定義

1.1.1　二項演算と半群

集合 S に対し, 写像 $\phi : S \times S \longrightarrow S$ を S 上の, または S に於ける **二項演算** という. 状況に応じ, $\phi(a,b) = a \cdot b, a+b, a \circ b$ 等と表すが, しばらくの間 $\phi(a,b) = a \cdot b = ab$ と表す.

$$a(bc) = (ab)c \quad (\forall a, b, c \in S)$$

を満たすとき, 二項演算は **結合法則** を満たすという.

空でない集合 S と, 結合法則を満たす二項演算 ϕ の組 $(S;\phi)$ を **半群** という.

$$a1 = 1a = a \quad (\forall a \in S)$$

を満たす $1 \in S$ が存在するとき, 1 を, 二項演算 ϕ に関する, S の **単位元** という. 単位元を持つ半群 $(S;\phi)$ を **単位半群** という. 文脈から演算が明らかな場合は, 演算を省略して, S を半群, 単位半群という.

例 1.1.1 自然数とその加法がなす半群を $(\mathbb{N};+)$ と表し, 自然数とその乗法がなす単位半群を $(\mathbb{N};\times)$ と表す.

例 1.1.2 空でない集合 X から自分自身への写像の全体を $\mathrm{Map}(X)$ と表す. $f, g \in \mathrm{Map}(X)$ に対し, 合成写像 $f \circ g$ を対応させる写像

$$\circ : \mathrm{Map}(X) \times \mathrm{Map}(X) \longrightarrow \mathrm{Map}(X)$$

は $\mathrm{Map}(X)$ 上の二項演算である. このとき, $(\mathrm{Map}(X);\circ)$ は, X の恒等写像 I_X を単位元とする単位半群である.

問 1.1.1 $(\mathrm{Map}(X);\circ)$ が単位半群をなすことを証明せよ.

半群 S の $n(\geq 3)$ 個の元 $a_1, \cdots, a_n$ の積を帰納的に

$$(a_1a_2)\, a_3 = a_1a_2a_3, \quad (a_1a_2 \cdots a_{n-1})a_n = a_1a_2 \cdots a_n$$

と定義する.

補題 1.1.2 $1 \leq n < m$ のとき

$$(a_1a_2 \cdots a_n)(a_{n+1}a_{n+2} \cdots a_m) = a_1a_2 \cdots a_m.$$

証明　$m-n$ に関する帰納法で示す. $m=n+1$ のとき, 定義より

$$(a_1\cdots a_n)a_{n+1}=a_1\cdots a_{n+1}.$$

$m=n+k$ $(k\geq 1)$ のとき正しいと仮定する. $m=n+(k+1)$ のとき

$$\begin{array}{lcll} a_1\cdots a_{n+k+1} & = & (a_1\cdots a_{n+k})a_{n+k+1} & \text{定義} \\ & = & ((a_1\cdots a_n)(a_{n+1}\cdots a_{n+k}))a_{n+k+1} & \text{帰納法の仮定} \\ & = & (a_1\cdots a_n)((a_{n+1}\cdots a_m)a_{n+k+1}) & \text{結合法則} \\ & = & (a_1\cdots a_n)(a_{n+1}\cdots a_{n+k+1}) & \text{定義} \end{array}.$$

従って, 帰納法により補題が示された. □

半群, 単位半群 S が **交換法則**：

$$ab=ba\quad(\forall a,b\in S)$$

を満たすとき, S を **可換半群**, **可換単位半群** という.

補題 1.1.3 S を可換半群とし, $a_1,\cdots,a_n\in S$ とする.

$$\sigma:\{1,2,\cdots,n\}\longrightarrow\{1,2,\cdots,n\}$$

を全単射とするとき,

$$a_1\cdots a_n=a_{\sigma(1)}\cdots a_{\sigma(n)}$$

が成り立つ.

証明　$n=2$ の場合は明らかである. $n-1\geq 3$ のときまで正しいとし, n の場合に示す. $\sigma(n)=n$ のときは明らか. $\sigma(k)=n$ $(k<n)$ とする.

$$\begin{aligned} a_{\sigma(1)}\cdots a_{\sigma(k-1)}a_{\sigma(k)}\cdots a_{\sigma}(n) &= a_{\sigma(1)}\cdots a_{\sigma(k-1)}a_{\sigma(k+1)}\cdots a_{\sigma(n-1)}a_{\sigma(k)}a_{\sigma(n)} \\ &= a_{\sigma(1)}\cdots a_{\sigma(k-1)}a_{\sigma(k+1)}\cdots a_{\sigma(n-1)}a_{\sigma(n)}a_{\sigma(k)} \\ &= (a_1\cdots a_{n-1})a_n \end{aligned}$$

となり, n の場合も正しい. 従って, 帰納法により補題が示された. □

半群 S に含まれる元の個数を $|S|$ で表し, S の**位数** という. $|S|$ が有限のとき, S を **有限半群** といい, $|G|=\infty$ のとき **無限半群** という.

(S,ϕ) を半群とし, T を S の部分集合とする. T の任意の二元 $a,b\in T$ に対し, $\phi(a,b)\in T$ が成り立つとき, 即ち, T の二項演算

$$\phi_T:T\times T\longrightarrow T;\quad (a,b)\longmapsto\phi(a,b)$$

が得られるとき, T は, ϕ に関して **閉じている** という. このとき, (T,ϕ_T) を半群 (S,ϕ) の **部分半群** という.

例 1.1.3 整数とその加法なす（単位可換）半群を $(\mathbb{Z};+)$ とすると, 自然数の集合 $\mathbb{N}$ は $+$ に関して閉じていて, $(\mathbb{N};+)$ は $(\mathbb{Z};+)$ の部分半群である. しかし, $(\mathbb{N};\times)$ は $(\mathbb{Z};+)$ の部分半群ではない.

1.1.2 群の定義

集合 G と, G に於ける二項演算の組 $(G;\phi)$ は, 次の (G1), (G2), (G3) を満たすとき**群** と呼ばれる. 煩雑なので, $\phi(a,b)$ を ab と表す.

(G1) (結合法則) $(ab)c = a(bc) \quad (\forall a,b,c \in G)$,

(G2) (単位元の存在)

$$a1 = 1a = a \quad (\forall a \in G)$$

を満たす $1 \in G$ が存在する. 1 を G の**単位元** という,

(G3) (逆元の存在) G の各元 a に対し

$$ab = ba = 1$$

を満たす $b \in G$ が存在する. b を a の **逆元** といい, a^{-1} と表す.

すなわち, 群 $(G;\phi)$ は単位半群であり, さらに, 各元の逆元が存在する. 演算を明示する必要がない場合, 演算を省略して, 群 $(G;\phi)$ を, G と略記する.

注意 1.1.1 単位元を e と表す場合もあるので, 他書を参照するときは注意せよ.

問 1.1.4 群 G の任意の元に対し, その逆元は唯一つであることを証明せよ.

群 G がさらに

(G4) (交換法則) $ab = ba \quad (\forall a,b \in G)$

を満たすとき, G は **アーベル群**, または **可換群** と呼ばれる.

アーベル群では演算を $a+b$ と加法の形で書くことが多い. 演算が加法のアーベル群を **加法群** ということもある. 加法群では単位元を 0 と書き **零元** という. また a の逆元を $-a$ と書き $a+(-b)$ を $a-b$ と書く. 一方, 演算が積の群を, **乗法群** ということもある.

例 1.1.4 有理数全体の集合 $\mathbb{Q}$ は, 加法に関して, 加法群をなす. また, 0 以外の有理数の集合 $\mathbb{Q}^\times$ は乗法に関して可換群をなす. 実数, 複素数に対しても同様なことが成り立つ.

例 1.1.5 複素数を成分に持つ n 次正則行列の全体を $\mathrm{GL}_n(\mathbb{C})$ と表す. A, B が正則行列ならば, AB も正則行列なので, 二項演算

$$\times : \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$$

を得る. このとき, $(\mathrm{GL}_n(\mathbb{C});\times)$ は単位行列 I_n を単位元とする群をなす. この群を n 次 **一般線形群** という. $A \in \mathrm{GL}_n(\mathbb{C})$ の逆元は A の逆行列 A^{-1} である. $\mathbb{C}$ を $\mathbb{R}$ または $\mathbb{Q}$ に置き換えても同様なことを得る.

例 1.1.6 X を空でない集合とする. X から X への全単射の全体を $\mathrm{Sym}(X)$ と表す. 写像の合成は $\mathrm{Sym}(X)$ の演算

$$\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \longrightarrow \mathrm{Sym}(X), \quad (\sigma, \tau) \mapsto \sigma \circ \tau$$

を定める. このとき, $(\mathrm{Sym}(X); \circ)$ は群をなす. この群を $\mathrm{Sym}(X)$ と略記し, X 上の **対称群** という.

問 1.1.5 $\mathrm{Sym}(X)$ が群をなすことを証明せよ.

例 1.1.7 $G_1, G_2, \cdots, G_n$ を n 個の群とし, これらの直積集合 G を考える：

$$G = G_1 \times G_2 \times \cdots \times G_n.$$

G の二元 $(a_1, a_2, \cdots, a_n)$, $(b_1, b_2, \cdots, b_n)$ に対し, その積を

$$(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$$

と定める. するとこの演算に関して, G は群をなし, 群 $G_1, G_2, \cdots, G_n$ の **直積** と呼ばれる. $(1, \cdots, 1)$ が単位元であり

$$(a_1, \cdots, a_n)^{-1} = (a_1^{-1}, \cdots, a_n^{-1})$$

である.

$G_1, \cdots, G_n$ がアーベル群, 特に加法群, の場合には, 直積 $G_1 \times G_2 \times \cdots \times G_n$ を **直和** といい

$$G_1 \oplus \cdots \oplus G_n$$

と表す.

問 1.1.6 $G = G_1 \times G_2 \times \cdots \times G_n$ が群をなすことを確かめよ.

例 1.1.8 整数のなす加法群 $\mathbb{Z}^+$ の n 個の直和

$$\mathbb{Z}^n := \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

は, 最も基本的なアーベル群のひとつである.

1.1.3 基本的性質

補題 1.1.7 G を群とするとき, 次が成立つ：

(1) 単位元は唯一つ存在する,

(2) $a \in G$ に対しその逆元は唯一つ存在する.

証明 (1) $1, 1'$ が共に単位元とすると, 単位元の性質から $1 = 1 \cdot 1' = 1' \cdot 1 = 1'$. (2) b, b' が共に a の逆元ならば $b = b1 = b(ab') = (ba)b' = 1b' = b'$. □

補題 1.1.8 （簡約法則）G を群とする．$a, b, c \in G$ に対し, 次が成り立つ.

$$ab = ac \Longrightarrow b = c, \quad ba = ca \Longrightarrow b = c.$$

証明 $a^{-1}(ab) = a^{-1}(ac)$ であり, 結合法則より $(a^{-1}a)b = (a^{-1}a)c$. 従って $b = c$. 後半も同様. □

補題 1.1.9 G を群とするとき, 次が成り立つ：

(1) $(ab)^{-1} = b^{-1}a^{-1}$,

(2) $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$,

(3) $(a^{-1})^{-1} = a$.

証明 (1) $(ab)(b^{-1}a^{-1}) = aa^{-1} = 1 = (b^{-1}a^{-1})(ab)$. 従って $b^{-1}a^{-1}$ は ab の逆元である．(2) は (1) を繰り返し用いればよい.
(3) $aa^{-1} = a^{-1}a = 1$ より, a は a^{-1} の逆元である． □

問 1.1.10 群 G の任意の元 a が $a^2 = 1$ を満たすならば, G は可換群であることを示せ.

$a \in G$, $n \in \mathbb{Z}$ に対し

$$a^n = \begin{cases} \overbrace{a \cdots a}^{n} & n > 0 \\ 1 & n = 0 \\ (a^{-1})^{-n} & n < 0 \end{cases}$$

と定める.

補題 1.1.11 m, n を任意の整数とする．このとき次が成り立つ.

(1) $(a^m)^{-1} = (a^{-1})^m$,

(2) $a^{m+n} = a^m a^n$,

(3) $(a^m)^n = a^{mn}$.

証明 (1) $m = 0$ のとき明らか. $m > 0$ のときは, 補題 1.1.9 (2) から得られる．$m < 0$ のとき, 定義と 補題 1.1.9 (2) より, 次を得る:

$$\begin{aligned} (a^m)^{-1} &= (\overbrace{a^{-1} \cdots a^{-1}}^{-m})^{-1} \\ &= \overbrace{(a^{-1})^{-1} \cdots (a^{-1})^{-1}}^{-m} \\ &= (a^{-1})^m. \end{aligned}$$

(2) $m, n \geq 0$ の場合は明らか.
（$m \geq 0, n < 0$ の場合）$m + n \geq 0$ ならば

$$a^m a^n = \overbrace{a \cdots a}^{m} \overbrace{a^{-1} \cdots a^{-1}}^{-n} = a^{m-(-n)} = a^{m+k}.$$

$m+n<0$ ならば $a^{m+n}=(a^{-1})^{-m-n}$.

$$a^m a^n = \overbrace{a\cdots a}^{m}\overbrace{a^{-1}\cdots a^{-1}}^{-n} = (a^{-1})^{-n-m} = a^{m+n}.$$

($m<0, n\geq 0$ の場合）も同様である.
($m,n<0$ の場合） $a^{m+n}=(a^{-1})^{-m-n}$,

$$a^m a^n = (a^{-1})^{-m}(a^{-1})^{-n} = (a^{-1})^{-m-n}.$$

以上で, (2) が示された.
(3) の証明は演習問題とする. □

問 1.1.12 補題 1.1.11 を証明せよ.

問 1.1.13 群 G の二元 a,b が, $ab=ba$ を満たすならば, $(ab)^n=a^nb^n$ が成り立つことを示せ.

例題 1.1.14 G を半群とする.

(G2') $\exists e\in G$ s.t. $ae=a$ $(\forall a\in G)$.

(G3') G の各元 a に対し, $\exists b\in G$ s.t. $ab=e$.

を満たすならば, G は群であることを示せ.

（解） 任意の $a\in G$ に対し, (G2') により $ae=a$. $ea=a$ を示そう. (G3') により $ab=e$ となる $b\in G$ が存在する. この b に対し, 再び (G3') を用いて, $bc=e$ となる $c\in G$ が存在する. このとき

$$a=ae=a(bc)=(ab)c=ec,\quad ea=e(ec)=(ee)c=ec=a.$$

従って $ae=ea=a$ $(\forall a\in G)$ となり, e は単位元である.
また

$$ba=b(ec)=(be)c=bc=e=ab.$$

従って b は a の逆元である. 以上で (G2),(G3) が確かめられ, G は群をなす. □

例題 1.1.15 半群 G は, 次を満たすとき群であることを証明せよ.

任意の元 a,b に対し, $ax=b, ya=b$ をみたす $x,y\in G$ が存在する.

（解） 前例題を利用して証明する. 仮定により, $a\in G$ に対し $ae=a$ となる e が存在する. また, a と, 任意の $b\in G$ に対し, $ca=b$ となる c が存在する. このとき

$$be=(ca)e=c(ae)=ca=b.$$

従って (G2') を満たす. さらに, 仮定により, 各 a に対し, $ab=e$ を満たす b が存在する. よって (G3') も満たされる. 従って, 前例題により, G は群である. □

問 1.1.16 有限半群 G は, 次を満たすならば群であることを示せ. G の任意の元 a,u,v に対し

(1) $au=av$ ならば $u=v$.

(2) $ua=va$ ならば $u=v$.

問 1.1.17 有限でない半群に対し, 上の問いは正しいか？

1.2 n 次対称群

1.2.1 n 文字の置換と n 次対称群

$I=\{1,2,\cdots,n\}$ 上の対称群 $(\mathrm{Sym}(I);\circ)$ を S_n と表し, n **次対称群** といい, S_n の元を n **文字の置換** と呼ぶ. 煩雑なので, $\sigma\circ\tau$ を $\sigma\tau$ と表し, 単位元を 1 と表す.

n 文字の置換 σ は, $1,2,\cdots,n$ の行き先がわかりさえすればよい. そこで σ を

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表す. このとき上の行の並べ方は任意でよい. 即ち $(i_1,i_2,\cdots,i_n)$ を $(1,2,\cdots,n)$ の任意の順列としたとき

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

も同じ置換 σ を表す. $\sigma(i)=i$ となるとき, その部分は省略してもよい. 例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 6 \\ 5 & 1 & 6 & 3 \end{pmatrix}.$$

n 文字の置換と $1,2,\cdots,n$ の順列が対応するので, n 文字の置換の個数, 即ち対称群 S_n の位数は $n!$ である：

補題 1.2.1 $|S_n|=n!$.

二つの置換

$$\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},\quad \tau=\begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

に対し

$$\sigma=\begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

と書き換えれば,

$$\sigma\tau=\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

と表される. また,

$$1=\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},\quad \sigma^{-1}=\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

と表される.

例 1.2.1

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

となるので

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

すなわち, S_n $(n \geq 3)$ において, 交換法則が成立たない.

例 1.2.2 σ, τ を上の通りとする. このとき

$$\tau^\sigma := \sigma\tau\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

即ち, 置換 τ^σ は τ の 1 行と 2 行を, それぞれ σ で置換したものに他ならない. 置換 τ^σ を τ に **共軛**（きょうやく）な置換という.

例 1.2.3 $n \leq m$ のとき, n 文字の置換は自然に m 文字の置換とみなせる.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & \cdots & m \\ i_1 & i_2 & \cdots & i_n & n+1 & \cdots & m \end{pmatrix}.$$

例 1.2.4 S_3 の元を

$$a_1 = 1,\ a_2 = (1\ 2),\ a_3 = (1\ 3),\ a_4 = (2\ 3),\ a_5 = (1\ 2\ 3),\ a_6 = (1\ 3\ 2)$$

とするとき, 積 $a_i a_j$ を (i, j) 成分とする表は次の通りである：

	1	a_2	a_3	a_4	a_5	a_6
1	1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	1	a_6	a_5	a_4	a_3
a_3	a_3	a_5	1	a_6	a_2	a_4
a_4	a_4	a_6	a_5	1	a_3	a_2
a_5	a_5	a_3	a_4	a_2	a_6	1
a_6	a_6	a_4	a_2	a_3	1	a_5

.

一般に有限群 G の元の積を上のように表したものを G の **乗積表** という.

1.2.2 巡回置換と互換

以下 $n \geq 2$ とする. n 文字の置換 σ が r 個の文字を

$$i_1 \to i_2 \to i_3 \to \cdots \to i_r \to i_1$$

のように移し, 他のものを動かさないとする. このとき σ を **長さ** r の **巡回置換** といい

$$(i_1\ i_2\ \cdots\ i_r)$$

と表す. 特に, 長さ 2 の巡回置換 $(i\ j)$ を **互換** という.
$(i_1\ i_2\ \cdots\ i_r)^{-1} = (i_r\ \cdots\ i_2\ i_1)$ であり, $(i\ j)^{-1} = (i\ j)$.

例 1.2.5

$$(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}.$$

例 1.2.6

$$(i\ j) = \begin{pmatrix} \cdots & i & \cdots & j & \cdots \\ \cdots & j & \cdots & i & \cdots \end{pmatrix}.$$

ここで $\cdots$ の所は, 上下に同じ文字が並ぶ.

定義から直ちに, 次を得る：

補題 1.2.2 σ, τ を互に共通文字を含まない巡回置換とするとき, $\sigma\tau = \tau\sigma$ が成り立つ.

問 1.2.3 補題 1.2.2 を確かめよ.

例 1.2.7 $\sigma = (i_1\ i_2\ \cdots\ i_r)$ を巡回置換とし,

$$\tau = \begin{pmatrix} i_1 & i_2 & \cdots & i_r & \cdots \\ j_1 & j_2 & \cdots & j_r & \cdots \end{pmatrix} \in S_n$$

とするとき

$$\sigma^\tau = \tau(i_1\ i_2\ \cdots\ i_r)\tau^{-1} = (j_1\ j_2\ \cdots\ j_r).$$

例 1.2.8

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 5 & 6 & 7 & 1 & 2 \end{pmatrix} = (1\,4\,6)(2\,3\,5\,7).$$

補題 1.2.4 n 文字の任意の置換は互に共通文字を含まない, いくつかの巡回置換の積として（順序を除いて）一意的に表される.

証明 まず一意性を n に関する帰納法で示そう.

$$\sigma = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s$$

と二通りに, 共通文字を含まない巡回置換の積として表されたとする. 補題 1.2.2 により, 1 は σ_1, τ_1 に含まれるとしてよい. このとき $\sigma_1 = \tau_1$ となる. 従って

$$\sigma_2 \cdots \sigma_r = \tau_2 \cdots \tau_s$$

となる. 帰納法の仮定により, $r = s$ であり, 順序を適当に変えれば, $\sigma_2 = \tau_2, \cdots, \sigma_r = \tau_r$ が成り立つ.

次に n 文字の任意の置換は互に共通文字を含まない, いくつかの巡回置換の積として表されることを, n に関する帰納法で証明する. $n=2$ のときは明らか. $k(\geq 2)$ のとき正しいと仮定する. $\sigma \in S_{k+1}$ を任意に取る.

$$\sigma(1)=i_1, \sigma(i_1)=i_2, \cdots, \sigma(i_r)=1, \quad i_j \neq 1 (1 \leq j \leq r)$$

となったとする. $r=k$ ならば, $\sigma=(1\ i_1\ i_2\ \cdots\ i_k)$ が成り立つ. $r<k$ のとき, $\sigma'=(i_r\ \cdots\ i_2\ i_1\ 1)\sigma$ は $1, i_1, \cdots, i_r$ を動かさないので, $k+1-(r+1)=k-r \leq k$ 文字の置換である. 帰納法の仮定から σ' は共通文字を含まない巡回置換 $\sigma_1, \cdots, \sigma_s$ の積として表される: $\sigma'=\sigma_1 \cdots \sigma_s$. 各々の σ_i は勿論文字 $1, i_1, \cdots, i_r$ を含まないので, $\sigma=(1\ i_1\ i_2\ \cdots\ i_k)\sigma_1 \cdots \sigma_s$ と, 互いに共通文字を含まない巡回置換の積として表された. □

問 1.2.5 S_4 の元を互いに共通文字を含まない巡回置換の積として表せ.

例 1.2.9 長さ 3 の巡回置換の二つの積は, 次の四通りである：

$$(a\ b\ c)(a\ b\ d)=(a\ c)(b\ d), \quad (a\ b\ c)(a\ d\ b)=(a\ d\ c)$$
$$(a\ b\ c)(a\ d\ e)=(a\ d\ e\ b\ c) \quad (a\ b\ c)(d\ e\ f)$$

ここで, a, b, c, d, e, f は互いに異なる文字とする.

例 1.2.10 巡回置換は, 互換の積として表されるが表し方は一通りではない：

$$(i_1\ i_2 \cdots i_r)=(i_1\ i_r)(i_1\ i_{r-1}) \cdots (i_1\ i_2), \quad (i\ j)=(1\ j)(1\ i)(1\ j).$$

補題 1.2.6 任意の n 文字の置換は, $n-1$ 個の互換

$$(1\,2), (1\,3), \ldots, (1\,n)$$

の幾つかの積として表される. 特に, n 文字の置換は互換の積として表される.

証明 $(i\,j)=(1\,j)(1\,i)(1\,j)$ なので, 補題 1.2.4 と例 1.2.10 より, 任意の置換は $n-1$ 個の互換 $(1\,2), (1\,3), \ldots, (1\,n)$ の幾つかの積として表されることが解る. □

$\sigma \in S_n$ を互いに共通文字を含まない巡回置換の積に表す：

$$\sigma=(a_{11}\ \cdots\ a_{1d_1})(a_{21}\ \cdots\ a_{2d_2}) \cdots (a_{r1}\ \cdots\ a_{rd_r}), \quad d_1 \geq d_2 \geq \cdots \geq d_r.$$

このとき

$$(d_1, d_2, \cdots, d_r)$$

を置換 σ の **型** という. 時に, $d_{s+1}=\cdots=d_r=1$ の部分を省略して, $(d_1, \cdots, d_s)$ を型という.

例 1.2.11 15 文字の置換 $(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9)(10\ 11)(12)(13)(14\ 15)$ の型は $(4,3,2,2,2)$ である.

例 1.2.12 4 文字の置換の型は,

$$(4),\ (3,1),\ (2,2),\ (2,1,1),\ (1,1,1,1)$$

の 5 通りある.

問 1.2.7 5 文字の置換の型の個数を求めよ.

補題 1.2.8 置換 $\sigma, \sigma' \in S_n$ が共役であるための必要十分条件は, それらの型が一致することである.

証明 σ と σ' が共役のとき, $\sigma' = \tau\sigma\tau^{-1}$ となる $\tau \in S_n$ が存在する. σ を巡回置換の積に分解し, 例 1.2.7 を適用すれば, σ と σ' の型が等しいことが解る. 逆に, σ, σ' の型が等しければ, 再び, 例 1.2.7 を用いて, $\sigma^\tau = \sigma'$ となる τ が作れる. □

1.2.3 偶置換と奇置換

定理 1.2.9 $n \geq 2$ とする. 置換 σ を互換の積として二通りに表されたとする：

$$\sigma = \tau_1 \cdots \tau_r = \tau'_1 \cdots \tau'_s.$$

このとき, $r \equiv s \pmod 2$[1].

証明 $I = \{1, 2, \cdots, n\}$ から互いに異なる元からなる集合 $\{i, j\}$ の全体を P とする：

$$P = \{\{i, j\} \mid 1 \leq i \neq j \leq n\}.$$

そこで,

$$\phi(\sigma) = \prod_{\{i,j\} \in P} (\sigma(i) - \sigma(j))(i - j)$$

の符号 $\mathrm{sign}(\phi(\sigma))$ を $\mathrm{sigm}(\sigma)$ と表す. とし,

$$\mathrm{sign}(\sigma) = \mathrm{sign}(\phi(\sigma)) = \begin{cases} 1 & (\phi(\sigma) > 0) \\ -1 & (\phi(\sigma) < 0) \end{cases}$$

と定める. すると, $\sigma, \tau \in S_n$ に対し, 次が成り立つ：

$$\begin{aligned}
\mathrm{sign}(\sigma\tau) &= \mathrm{sign}\left(\prod_{\{i,j\} \in P} ((\sigma\tau)(i) - (\sigma\tau)(j))(i - j) \right) \\
&= \mathrm{sign}\left(\prod_{\{i,j\} \in P} ((\sigma\tau)(i) - (\sigma\tau)(j))(\tau(i) - \tau(j))(\tau(i) - \tau(j))(i - j) \right) \\
&= \mathrm{sign}\left(\prod_{\{i,j\} \in P} ((\sigma\tau)(i) - (\sigma\tau)(j))(\tau(i) - \tau(j)) \right) \mathrm{sign}\left(\prod_{\{i,j\} \in P} (\tau(i) - \tau(j))(i - j) \right) \\
&= \mathrm{sign}(\sigma)\mathrm{sign}(\tau).
\end{aligned}$$

τ が互換ならば, $\mathrm{sign}(\tau) = -1$ が得られる. 従って,

$$\mathrm{sign}(\sigma) = (-1)^r = (-1)^s$$

[1] 整数 a, b に対し, $a - b$ が偶数のとき, $a \equiv b \pmod 2$ と表す.

となり, $r \equiv s \pmod 2$ を得る. □

置換 σ に対し, $\mathrm{sign}(\sigma) = \mathrm{sign}(\phi(\sigma))$ を σ の **符号** という. $\mathrm{sign}(\sigma) = 1$ となる置換 σ を **偶置換** といい, $\mathrm{sign}(\sigma) = -1$ となる置換 σ を **奇置換** という.

定理の証明より, 次を得る：

系 1.2.10 偶置換は偶数個の互換の積として表され, 奇置換は奇数個の互換の積として表される. また, 置換 $\sigma, \tau \in S_n$ に対し,

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)$$

が成り立つ.

例 1.2.13 長さ k の巡回置換 σ に対し, $\mathrm{sign}(\sigma) = (-1)^{k-1}$. すなわち, 長さが偶数の巡回置換は奇置換であり, 長さが奇数の巡回置換は偶置換である.

1.3　部分群と剰余類

1.3.1　部分群の定義

H を群 G の部分集合とする. 次が満たされるとき H を G の**部分群** といい,

$$H \leq G$$

と表す.

(SG0)] $1 \in H$.

(SG1) $a, b \in H \Longrightarrow ab \in H$.

(SG2) $a \in H \Longrightarrow a^{-1} \in H$.

問 1.3.1 H を群 G の部分群とする. このとき, H は群をなすことを確かめよ.

例 1.3.1 G 自身, 或いは単位元だけからなる集合 $\{1\}$ は常に部分群であり, **自明な部分群** と呼ばれる：

$$G \leq G, \quad \{1\} \leq G.$$

また G 以外の部分群 H を **真部分群** といい, $H < G$ と表す.

例 1.3.2 正の実数のなす乗法群 $(\mathbb{R}^\times_{>0}; \cdot)$ は 0 以外の実数のなす乗法群 $\mathbb{R}^\times$ の部分群である. しかし, $(\mathbb{R}^\times_{>0}, \cdot)$ は, その演算が実数のなす加法群 $\mathbb{R}^+ = (\mathbb{R}; +)$ の演算から導かれたものではないので, $\mathbb{R}^+$ の部分群ではない.

問 1.3.2 絶対値が 1 の複素数全体の集合を $\mathbb{C}^\times_1$ と表す. $\mathbb{C}^\times_1 < \mathbb{C}^\times$ を示せ.

例 1.3.3 $z^n = 1$ を満たす複素数 z を 1 の n 乗根という. 1 の n 乗根全体は, 積に関して位数 n のアーベル群をなす. この群を μ_n と表す：

$$\mu_n = \left\{ \cos\left(\frac{2k\pi}{n}\right) + \sqrt{-1}\sin\left(\frac{2k\pi}{n}\right) \;\middle|\; 0 \leq k \leq n-1 \right\}, \quad \mu_n < \mathbb{C}_1^{\times}.$$

例 1.3.4 行列式が 1 である実係数 n 次行列の全体のなす集合を $\mathrm{SL}_n(\mathbb{R})$ で表すと, $\mathrm{SL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R})$.

例 1.3.5 n 文字の置換

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

を $n+m$ 文字の置換

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & \cdots & n+m \\ i_1 & i_2 & \cdots & i_n & n+1 & \cdots & n+m \end{pmatrix}$$

とみなせば, S_n は S_{n+m} の部分群となる.

例 1.3.6 $n(\geq 2)$ 文字の偶置換全体は, S_n の部分群をなす. これを A_n と表し n 次の**交代群** という. A_n の位数は $n!/2$ である.

問 1.3.3 $A_n < S_n$ を確かめ, $|A_n| = n!/2$ を示せ.

例 1.3.7 $i = 1, 2$ に対し, H_i が G_i の部分群ならば, $H_1 \times H_2$ は自然に $G_1 \times G_2$ の部分群とみなせる.

後々便利なので, 次の記法を導入する. 群 G の部分集合 S, T に対し

$$ST = \{st \mid s \in S,\ t \in T\}, \quad S^{-1} = \{s^{-1} \mid s \in S\}$$

と定める. 特に S が一つの元 s からなるとき, $\{s\}T = sT, \quad T\{s\} = Ts$ と表す. 加法群の場合は, 次のように定める:

$$S + T = \{s + t \mid s \in S, t \in T\}, \quad -S = \{-s \mid s \in S\}, \quad \{s\} + T = s + T, \quad T + \{s\} = T + s.$$

定義から, 次を得る：

補題 1.3.4 G を群とし, R, S, T を G の部分集合とする. このとき, 次が成り立つ：

(1) $(RS)T = R(ST)$,

(2) $(RS)^{-1} = S^{-1}R^{-1}$.

補題 1.3.5 H を群 G の部分群とし, $h \in H$ とする. このとき, 次が成り立つ：

$$hH = Hh = H = H^{-1}.$$

補題 1.3.6 H を群 G の空でない部分集合とするとき, 次が成り立つ.

$$H \leq G \iff HH \subset H,\ H^{-1} \subset H \iff HH = H,\ H^{-1} = H.$$

問 1.3.7 補題 1.3.4, 1.3.5, 1.3.6 を証明せよ.

補題 1.3.8 H, K を群 G の部分群とするとき, 次が成り立つ：

$$HK = KH \iff HK \leq G.$$

証明 $HK = KH$ を仮定する. このとき, $1 = 1.1 \in HK$ であり,

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK,$$

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK.$$

従って, 補題 1.3.6 により, $HK \leq G$ である. 逆に HK が部分群ならば, $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ が成り立つ. □

次の補題は, 証明は易しいが, 有用である：

補題 1.3.9 G を群とし, $H \leq G$ とする. 部分集合 $U \subset G$, $V \subset H$ に対し,

$$UV \cap H = (U \cap H)V$$

が成り立つ.

証明 $UV \cap H \supset (U \cap H)V$ はよい. $uv = h \in UV \cap H$ とすると, $u = hv^{-1} \in H$ なので, $UV \cap H \subset (U \cap H)V$ が成り立つ. □

1.3.2　部分集合が生成する部分群

部分群の定義より, 次を得る.

補題 1.3.10 $\{H_i\}_{i \in I}$ を群 G の部分群の集りとするとき,

$$\cap_{i \in I} H_i$$

は部分群であり, 全ての H_i $(i \in I)$ に含まれる G の最大の部分群である.

問 1.3.11 補題 1.3.10 を証明せよ.

群 G の部分集合 S に対し, S を含む G の最小の部分群を $\langle S \rangle$ と表し, S により **生成された部分群** という. また, $G = \langle S \rangle$ となるとき, S を G の **生成系** という.

命題 1.3.12 S を群 G の部分集合とし, S を含む G の部分群全体の集合を $\{H_i \mid i \in I\}$ とする. このとき, 次が成り立つ：

$$\langle S \rangle = \{s_1 s_2 \cdots s_n \mid s_i \in S \cup S^{-1}, n = 0, 1, 2, \cdots\} = \cap_{i \in I} H_i.$$

但し, 0 個の積は単位元を表すとする.

証明 真ん中の集合を H とおく. すると, H は G の部分群をなし, 明らかに, S を含む. 従って, 定義から, $\langle S\rangle \subset H$. $S \subset H_i$ であり, H_i は部分群なので, $H \subset H_i$. 従って $H \subset \cap_{i\in I} H_i$. S を含む任意の部分群 K に対し, $\{H_i\}$ の定義から, K はある H_j に一致している. よって $\cap_{i\in I} H_i \subset K$. 従って, $\cap_{i\in I} H_i$ は S を含む最小の部分群となり, $\langle S\rangle$ に一致する. □

$a, a_1, \cdots, a_n$ を群 G の元とする. $S = \{a_1, \cdots, a_n\}$ のとき, $\langle S\rangle = \langle a_1, \cdots, a_n\rangle$ と表す. 特に, $\langle a\rangle$ を a が生成する **巡回部分群** という.

例 1.3.8 G を群とし, $a \in G$ とする. このとき

$$\langle a\rangle = \{\cdots, a^{-2}, a^{-1}, a^0 = 1, a^1, a^2, a^3, \cdots\}.$$

例 1.3.9

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Z} \right\}$$

は $\mathrm{GL}_2(\mathbb{Z})$ の無限巡回部分群である.

例 1.3.10 S_4 の部分群 $V_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ は $V_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ と表される.

例 1.3.11 整数のなす加法群 $\mathbb{Z}^+$ では, 記法を少しかえる：$a_1, \cdots, a_r \in \mathbb{Z}$ に対し

$$(a_1, \cdots, a_r) := \langle a_1, \cdots, a_r\rangle = \{c_1a_1 + \cdots + c_ra_r \mid c_i \in \mathbb{Z}\ (i = 1, \cdots, r)\}.$$

$a_1, \cdots, a_r$ のうち少なくとも一つは 0 でないとし, それらの最大公約数を d とする. このとき,

$$(d) = (a_1, \cdots, a_r).$$

問 1.3.13 上の例を確かめよ.

命題 1.3.14 (1) $n \geq 2$ のとき,

$$\begin{aligned} S_n &= \langle (1\ 2), (1\ 3), \cdots, (1\ n)\rangle = \langle (1\ 2), (2\ 3), \cdots, (n-1\ n)\rangle \\ &= \langle (1\ 2\ 3\ \cdots\ n), (1\ 2)\rangle, \\ A_n &= \langle (1\ i)(1\ j) \mid 2 \leq i < j \leq n\rangle. \end{aligned}$$

(2) $n \geq 3$ のとき,

$$A_n = \langle (1\ 2\ i) \mid 3 \leq i \leq n\rangle = \langle (1\ 2\ 3), (1\ 2)(3\ 4), \cdots, (1\ 2)(n-1\ n)\rangle.$$

(3) $n \geq 5$ ならば, $A_n = \langle (i\ j)(k\ l) \mid i, j, k, l(\neq)\rangle$[2]

[2] $a, b, \cdots, x(\neq)$ は, $a, b, \cdots, x$ が互いに異なることを意味する.

証明　(1) 最初の等式は, 補題 1.2.6 から, 直ちに得られる. $(1\ i)(i\ i+1)(1\ i) = (1\ i+1)$ なので, $i = 1, 2, \cdots$ として,

$$(1\ 2), (1\ 3), \cdots \in \langle (i\ i+1) \mid 1 \leq i \leq n-1 \rangle \leq S_n.$$

よって, 二番目の等式を得る. $\sigma = (1\ 2\ 3\ \cdots\ n)$ とおくと, 補題 1.2.7 を用いて,

$$(1\ 2)^{\sigma^i} = (i+1\ i+2).$$

よって, 三番目の等式を得る. 四番目の等式は, 最初の等式から得られる.
(2) $n = 3$ のときは良い. $n > 3$ とする. $1 < i \neq j$ ならば, $(1\ i)(1\ j) = (1\ j\ i)$. よって, $2 < i$ ならば, $(1\ 2)(1\ i) = (1\ 2\ i)^{-1}$. $2 < i < j$ ならば,

$$(1\ i)(1\ j) = (1\ i)(1\ 2)(1\ 2)(1\ j) = (1\ 2\ i)(1\ 2\ j)^{-1}.$$

よって, (1) の四番目の等式から, 最初の等式を得る. 次に, $i > 2$ のとき,

$$(1\ 2\ i)^{-1} = (1\ 2)(1\ i) \in \langle (1\ 2\ 3), (1\ 2)(3\ 4), \cdots, (1\ 2)(n-1\ n) \rangle$$

を, i に関する帰納法で示す. $i = 3$ のときは良い. $i > 3$ とすると,

$$(1\ 2)(1\ i+1) = (1\ 2)(1\ i)(i\ i+1)(1\ i) = (1\ 2)(1\ i)(i\ i+1)(1\ 2)(1\ 2)(1\ i).$$

よって, 帰納法により, 上の主張が示され, 二番目の等式を得る.
(3) $n \geq 5$ のとき, 長さ 3 の任意の巡回置換 $(i\ j\ k)$ に対し, $i, j, k, l, m(\neq)$ となる l, m が存在する. このとき

$$(i\ j\ k) = (i\ j)(l\ m)(l\ m)(j\ k)$$

なので, A_n は $(2, 2)$ 型の置換で生成される. □

例 1.3.12　uv 平面の角 $2\pi/n$ の回転を $x = \rho_n$ と表し, u 軸に関する角 π の回転を $y = r$ と表す. このとき,

$$D_{2n} = \langle x, y \rangle \leq \mathrm{O}_2(\mathbb{R})$$

を位数 $2n$ の **二面体群** という.

$$x^n = 1, \quad y^2 = 1, \quad yxy^{-1} = x^{-1}$$

が成り立ち,

$$D_{2n} = \{1, x, \cdots, x^{n-1}\} \cup \{y, yx, \cdots, yx^{n-1}\}.$$

問 1.3.15　上の例を確かめよ.

1.3.3 巡回群

G を群とする. $a \in G$ に対し, $a^n = 1$ となる最小の自然数 n を **元 a の位数** といい,

$$n = \mathrm{ord}(a)$$

と表す. $a^n = 1$ を満たす自然数が存在しないとき, a の位数は無限であるという.

例 1.3.13 任意の群 G に対し, 単位元 1 の位数は 1. n 次の対称群 S_n において, 互換の位数は 2, 長さ k の巡回置換の位数は k.

例 1.3.14 $\mathrm{ord}(a) = \infty$ ならば

$$\langle a \rangle = \{\cdots, a^{-n}, \cdots, a^{-1}, a^0 = 1, a^1, \cdots, a^m, \cdots\}, \quad a^i \neq a^j \ (i \neq j).$$

$\mathrm{ord}(a) < \infty$ ならば, $a^i = a^j$ $(\exists i, j \in \mathbb{Z})$. 従って $a^l = 1$ $(\exists l \in \mathbb{N})$.

問 1.3.16 a, b を群 G の二元とする. ab の位数が有限ならば, $\mathrm{ord}(ab) = \mathrm{ord}(ba)$ が成り立つことを示せ.

補題 1.3.17 群 G の元 a の位数を n $(< \infty)$ とするとき, 次が成り立つ.

(1) $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ であり, $a^i \neq a^j$ $(0 \leq i < j \leq n-1)$. 特に, $n = \mathrm{ord}(a) = |\langle a \rangle|$.

(2) $a^m = 1$ ならば, m は $n = \mathrm{ord}(a)$ の倍数である.

証明 (1) の右辺が左辺に含まれるのは良い. 逆に a^m $(m \in \mathbb{Z})$ を左辺から任意にとる. m を n で割った商を q, 余りを r とすると $m = qn + r$ $(r < n)$ と表される. すると,

$$a^m = (a^n)^q a^r = a^r. \tag{1.1}$$

従って, a^m は, (1) の右辺に含まれる. また, $a^i = a^j$ $(0 \leq i < j \leq n-1)$ とすれば, $a^{j-i} = 1$ で $0 < j - i < n$ となり n のとり方に反する. 従って, (1) を得る. $a^m = 1$ ならば, (1.1) において, $r = 0$ となり, $n|m$ を得る. □

群 G は $G = \langle a \rangle$ $(\exists a \in G)$ と表されるとき, **巡回群** と呼ばれ, a を巡回群 G の **生成元** という.

例 1.3.15 n を自然数とするとき, 1 の n 乗根全体のなす群 μ_n は, $e^{\frac{2\pi i}{n}}$ を生成元とする位数 n の巡回群である.

例 1.3.16 整数のなす加法群 $\mathbb{Z}^+$ は無限巡回群であり, その生成元は 1 と -1 の二つである.

補題 1.3.18 C_m, C_n を位数 m, n の巡回群とする, m, n が互いに素ならば, 直積 $C_m \times C_n$ は位数 mn の巡回群である.

証明 $C_m = \langle a \rangle, C_n = \langle b \rangle$ とするとき, $(a, b) \in C_m \times C_n$ の位数は mn であることを示そう. $(a, b)^l = (a^l, b^l) = (1, 1)$ とすると, $m|l, n|l$, m, n が互いに素なので, $mn|l$, 一方 $(a, b)^{mn} = (1, 1)$. さて, $\langle (a, b) \rangle \subset C_m \times C_n$ であり, これらの群の位数は共に mn なので等しい, すなわち $C_m \times C_n$ は (a, b) を生成元とする巡回群である. □

例 1.3.17 C_2 を位数 2 の巡回群とする．このとき $C_2 \times C_2$ は位数 4 のアーベル群であるが巡回群ではない．この群を Klein **の四元群** という．

補題 1.3.19 $C = \langle a \rangle$ を位数 $n\ (< \infty)$ の巡回群とし，n の任意の約数 $m \geq 1$ に対し，

$$C^{(m)} = \{g \in C \mid g^m = 1\}$$

とする．このとき

$$C^{(m)} = \langle a^{\frac{n}{m}} \rangle$$

であり，これは位数 m の唯一つの部分群である．

証明　$b = a^{\frac{n}{m}}$ とするとき，$\mathrm{ord}(b) = m$ を示そう．$b^m = a^{\frac{n}{m}m} = a^n = 1$ が成り立つ．一方 $b^l = 1$ とすると $b^l = a^{\frac{n}{m}l} = 1$. 故に，$n|\frac{ln}{m}$ となり，$m|l$ を得る．従って $\mathrm{ord}(b) = m$ である．

次に $C^{(m)} = \langle b \rangle$ を示す．定義により，$C^{(m)} \supset \langle b \rangle$. 逆に，任意の $c \in C^{(m)}$ を採る，$c = a^l$ と表され，$c^m = a^{lm} = 1$ なので，$n|lm$. 従って，$\frac{n}{m}|l$ となり，$c = a^l \in \langle a^{\frac{n}{m}} \rangle$. よって，$C^{(m)} \subseteq \langle b \rangle$ を得て，$C^{(m)} = \langle b \rangle$.

最後に一意性を示そう．H を位数 m の任意の部分群とする．H の任意の元 d は $d^m = 1$ を満たすので，$d \in C^{(m)}$. 従って $H \leq C^{(m)}$. 双方の位数は，共に m なので $H = C^{(m)}$. □

自然数 n に対し，

$$\varphi(n) = \#\{i \in \{1, 2, \cdots, n\} \mid ((i, n) = 1\}$$

を **オイラーの** φ **関数** という．

補題 1.3.20 $C = \langle a \rangle$ を位数 n の巡回群とする．このとき a^k が C の生成元であるための必要かつ十分条件は n と k が互いに素となることである．特に，C の生成元の個数は $\varphi(n)$ に等しい．

証明　a^k を生成元とする．すなわち，$\langle a^k \rangle = C$ とする．このとき $a = (a^k)^l\ (\exists l \in \mathbb{Z})$ と表される．$a^{kl-1} = 1$ となるので $n|kl - 1$. 従って n, k の公約数は 1 に限る．逆に $(n, k) = 1$ とすれば

$$nu + kv = 1, \quad \exists u, v \in \mathbb{Z}$$

と表される．すると，$a = a^1 = a^{nu+kv} = (a^k)^v$ となり，$\langle a^k \rangle = C$. □

巡回群を利用して，Euler の関数 $\varphi(m)$ に係る，次の関係式を証明する：

補題 1.3.21 n を正の整数とするとき

$$n = \sum_{m|n} \varphi(m)$$

が成立つ．ただし，和は n の約数全てについての和である．

証明 $C = \langle a \rangle$ を位数 n の巡回群とする. n の約数 m に対し, 位数 m の元の集合を $O(m)$ とおく. このとき

$$C = \sum_{m|n} O(m) \tag{1.2}$$

が成り立つ. 実際, 右辺の各々は互いに交わらず, 左辺に含まれることはよい. 逆に a^k を左辺からとれば, $(a^k)^n = 1$ なので, 補題 1.3.17 より, a^k の位数 m は n の約数となり, $a^k \in O(m)$.

$O(m)$ は位数 m の部分群 $C^{(m)}$ の生成元の集合に一致するので, 補題 1.3.20 により, $|O(m)| = \varphi(m)$. 従って (1.2) の両辺の個数をとれば

$$n = |C| = \sum_{m|n} \varphi(m)$$

を得る. □

定理 1.3.22 （巡回群の特徴づけ）G を有限群とする. 任意の自然数 m に対し, 部分集合

$$G^{(m)} = \{g \in G \mid g^m = 1\}$$

に含まれる元の個数が m 以下ならば, G は巡回群である.

証明 G の位数を n とする. 位数 m の元の集合を $O(m)$ とおく. このとき

$$G = \sum_{m|n} O(m). \tag{1.3}$$

定義より, $O(m) \subseteq G^{(m)}$ である. $O(m) \neq \emptyset$ とする. $a \in O(m)$ とすると $\langle a \rangle \subseteq G^{(m)}$. $m = |\langle a \rangle| \leq |G^{(m)}| \leq m$ なので, $G^{(m)}$ は位数 m の巡回群であり, $O(m)$ はその生成元の集合である. 従って

$$O(m) \neq \emptyset \quad \Longrightarrow \quad |O(m)| = \varphi(m).$$

(1.3) の両辺の個数を比べ

$$n = \sum_{m} \varphi(m).$$

ここで, 和は $O(m) \neq \emptyset$ を満たす n の約数 m についての和である. 一方, 補題 1.3.21 により

$$n = \sum_{m|n} \varphi(m).$$

従って n の任意の約数に対し $O(m) \neq \emptyset$ でなければならない. 特に $O(n) \neq \emptyset$ となり, $n = \mathrm{ord}(g)$ となる $g \in G$ が存在し, $G = \langle g \rangle$ となる. □

定理 1.3.23 体 k の乗法群 $k^\times$ の有限部分群 G は巡回群である.

証明 体[3] k における, 方程式 $X^m = 1$ の解の個数は, 定理 **??** より, 高々 m 個である. 従って $|G^{(m)}| \leq m$. よって, 定理 1.3.22 により, G は巡回群である. □

[3]体の定義に関しては, 次章を参照せよ.

1.3.4 剰余類と Lagrange の定理

G を群, H をその部分群とする. G の二元 a と b は,

$$a^{-1}b \in H \quad (ab^{-1} \in H)$$

が成り立つとき, H に関して **左合同**（**右合同**）といい,

$$a \equiv b \pmod{H} \quad (a \equiv_r b \pmod{H})$$

と表す. 左合同（右合同）という関係は同値関係である.

問 1.3.24 左合同という関係は同値関係であること, 即ち, 次の (1),(2),(3) を満たすことを示せ.

(1) （反射律）$a \equiv a \pmod{H} \quad (\forall a \in G)$.

(2) （対称律）$a \equiv b \pmod{H} \Longrightarrow b \equiv a \pmod{H}$.

(3) （推移律）$a \equiv b \pmod{H}, b \equiv c \pmod{H} \Longrightarrow a \equiv c \pmod{H}$.

例 1.3.18 $H = \{1\}$ のとき

$$a \equiv b \pmod{H} \quad \Longleftrightarrow \quad a = b.$$

（上の同値関係に関して） $a \in G$ を含む同値類

$$aH = \{b \in G \mid b \equiv a \pmod{H}\}, \quad Ha = \{b \in G \mid a \equiv_r b \pmod{H}\}$$

を, それぞれ a を含む **左剰余類**, **右剰余類** という. 以下, 左合同に関して議論を進めるが, 右合同に関しても相応の結果が成り立つ.

二つの剰余類が一致する為の条件として, 次を得る：

補題 1.3.25 $aH = bH \quad \Longleftrightarrow \quad b^{-1}a \in H \quad \Longleftrightarrow \quad a^{-1}b \in H \quad \Longleftrightarrow \quad aH \cap bH \neq \emptyset$.

問 1.3.26 補題を証明せよ.

写像

$$H \longrightarrow aH, \quad h \mapsto ah \tag{1.4}$$

は全単射なので, $|aH| = |H|$. 即ち, 剰余類に含まれる元の個数は互いに等しい.

H の左剰余類全体の集合 $\{a_iH\}_{i \in I}$ は, 補題より, G の分割を与えることがわかる：

$$G = \sum_{i \in I} a_iH \quad (\Longleftrightarrow \ G = \cup_{i \in I} a_iH, \ a_iH \cap a_jH = \emptyset \ (i \neq j)). \tag{1.5}$$

この分割を G の H による **左剰余類分割** といい, 各剰余類から元を一つずつ選びその全体の集合 $\{a_i\}_{i\in I}$ を **左完全代表系**という. また左剰余類全体の集合を G/H で表す：

$$G/H = \{a_iH \mid i \in I\}.$$

全く同様に, 右剰余類分割, 右完全代表系が定義される. 右剰余類の集合を $H\backslash G$ と表す. 可換群では, 左剰余類と右剰余類は一致する.

例 1.3.19 $m > 1$ を自然数とする. $\mathbb{Z}^+$ の部分群 (m) に対し, 整数 r を含む剰余類を $[r]$ と表す：

$$\mathbb{Z}/(m) = \{[0], [1], \cdots, [m-1]\}.$$

$0 \le i \le m-1$ に対し, $[i] = i + (m) = \{i + am \mid a \in \mathbb{Z}\}$ は, m で割ったとき余りが i となる整数全体の集合であり, 剰余類と呼ばれる所以である.

例 1.3.20 一般には, $aH = Ha$ は成り立たない. 例えば, $H = \langle(1\ 2)\rangle \le S_3$ のとき,

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \quad H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}.$$

例 1.3.21 $n \ge 2$ とする. S_n において, A_n の左剰余類は A_n, $(1\ 2)A_n$ の二つで, $(1\ 2)A_n$ は n 文字の奇置換全体の集合である. また右剰余類は A_n, $A_n(1\ 2)$ であり, $(1\ 2)A_n = A_n(1\ 2)$.

例 1.3.22 S_4 において V_4 （例 1.3.10 参照） の左剰余類は, 次の 6 個である.

$$\begin{aligned}
V_4 &= \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},\\
(1\ 2)V_4 &= \{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\},\\
(1\ 3)V_4 &= \{(1\ 3), (1\ 2\ 3\ 4), (2\ 4), (1\ 4\ 3\ 2)\},\\
(1\ 4)V_4 &= \{(1\ 4), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (2\ 3)\},\\
(1\ 2\ 3)V_4 &= \{(1\ 2\ 3), (1\ 3\ 4), (3\ 2\ 4), (1\ 4\ 2)\},\\
(1\ 2\ 4)V_4 &= \{(1\ 2\ 4), (1\ 4\ 3), (1\ 3\ 2), (2\ 3\ 4)\}.
\end{aligned}$$

従って

$$\{1, (1\ 2), (1\ 3), (1\ 4), (1\ 2\ 3), (1\ 2\ 4)\}$$

は左剰余類 の左完全代表系である.

補題 1.3.27 H を群 G の部分群とし, $\{a_i\}_{i\in I}$ を一組の左完全代表系とするとき, $\{a_i^{-1}\}_{i\in I}$ は右完全代表系である. 特に $|G/H| = |H\backslash G|$ を得る.

証明

$$G = \sum_{i\in I} a_iH$$

なので

$$G = G^{-1} = \sum_{i\in I}(a_iH)^{-1} = \sum_{i\in I} H^{-1}a_i^{-1} = \sum_{i\in I} Ha_i^{-1}.$$

この等式は, $\{a_i^{-1}\}$ が右完全代表形であることを示す. □

例 1.3.23 $H = \langle (1\ 2) \rangle \leq S_3$ のとき, H の左剰余類は

$$H = \{1, (1\ 2)\},\ (1\ 3)H = \{(1\ 3), (1\ 2\ 3)\},\ (2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$$

であり, 右剰余類は

$$H = \{1, (1\ 2)\},\ H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\},\ H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}.$$

群 G の部分群 H に対し,

$$|G : H| := |G/H| = |H\backslash G|$$

を H の G における **指数** という.

定理 1.3.28 （Lagrange の定理 ）H を有限群 G の部分群とするとき

$$|G| = |G : H||H| = |G/H||H|$$

が成立つ.

証明 $\{a_1, \cdots, a_n\}$ をひと組の左完全代表系とすると, 補題 1.5 より

$$G = a_1H + \cdots + a_nH.$$

また, $|H| = |a_1H| = \cdots = |a_nH|$ なので

$$|G| = |a_1H| + \cdots + |a_nH| = n|H| = |G : H||H|$$

を得る. □

定理より直ちに次を得る.

系 1.3.29 H を有限群 G の部分群とするとき, $|H|$ は $|G|$ の約数である.

系 1.3.30 G を位数 n の有限群とする. このとき

$$\mathrm{ord}(a)|n, \quad a^n = 1, \quad (\forall a \in G)$$

が成り立つ.

証明 元 a の位数 $\mathrm{ord}(a)$ は a で生成された部分群 $\langle a \rangle$ の位数である：$\mathrm{ord}(a) = |\langle a \rangle|$. 上の系により, $n = \mathrm{ord}(a)n'$ $(\exists n' \in \mathbb{N})$ と表される. 従って, $a^n = a^{\mathrm{ord}(a)n'} = 1$. □

系 1.3.31 $K \leq H \leq G$ のとき,

$$|G : K| = |G : H||H : K|.$$

証明

$$G = \sum_{i \in I} Ha_i, \quad H = \sum_{j \in J} Kb_j$$

とするとき

$$G = \sum_{i \in I} Ha_i = \sum_{i \in I} \sum_{j \in J} Kb_j a_i = \sum_{(i,j) \in I \times J} Kb_j a_i.$$

よって

$$|G : K| = |I \times J| = |I||J| = |G : H||H : K|.$$

□

例 1.3.24 4 次の対称群 S_4 の部分群をすべて書き出そう. $|S_4| = 4! = 24$ なので, Lagrange の定理により, 部分群の位数は

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 8, \quad 12, \quad 24$$

のいずれかである.

位数 1 $\{1\}$.

位数 2 $\{1, (1\ 2)\}$, $\{1, (1\ 3)\}$, $\{1, (1\ 4)\}$, $\{1, (2\ 3)\}$, $\{1, (2\ 4)\}$, $\{1, (3\ 4)\}$, $\{1, (1\ 2)(3\ 4)\}$, $\{1, (1\ 3)(2\ 4)\}$, $\{1, (1\ 4)(2\ 3)\}$.

位数 3 $\langle (1\ 2\ 3) \rangle$, $\langle (1\ 2\ 4) \rangle$, $\langle (1\ 3\ 4) \rangle$, $\langle (2\ 3\ 4) \rangle$.

位数 4 $\{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$, $\{1, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$, $\{1, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}$, $V_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\langle (1\ 2\ 3\ 4) \rangle$, $\langle (1\ 2\ 4\ 3) \rangle$, $\langle (1\ 3\ 2\ 4) \rangle$.

位数 6 $S(\{1, 2, 3\}) = S_3$, $S(\{1, 2, 4\})$, $S(\{1, 3, 4\})$, $S(\{2, 3, 4\})$.

位数 8 $\langle (1\ 2\ 3\ 4), (1\ 3) \rangle = \{1, (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}$, $\langle (1\ 2\ 4\ 3), (1\ 4) \rangle$, $\langle (1\ 3\ 2\ 4), (1\ 2) \rangle$.

位数 12 A_4.

位数 24 S_4.

問 1.3.32 素数位数の群 G は, $\{1\}, G$ 以外に部分群を含まないことを示せ.

問 1.3.33 $|G : H|$ が素数のとき, $H < K < G$ となる部分群 K は存在しないことを示せ.

問 1.3.34 H, K を位数 m, n の群とする. $(m, n) = 1$ のとき, $H \cap K = \{1\}$ であることを示せ.

1.4　正規部分群と剰余群

1.4.1　正規部分群

群 G の部分群 N は,

(NSG) $xN = Nx \quad (\forall x \in G)$

を満たすとき, N を G の **正規部分群** といい,

$$N \trianglelefteq G$$

と表す.

問 1.4.1 $N \trianglelefteq G$ とする. このとき, 任意の部分集合 $S \subset G$ に対し, $SN = NS$ が成り立つことを示せ.

例 1.4.1 アーベル群の部分群はすべて正規部分群である.

非自明な正規部分群を持たない群で $\{1\}$ と異なる群を **単純群** という.

補題 1.4.2 可換単純群は素数位数の巡回群であり, 逆に, 素数位数の群は可換単純群である.

証明　G を可換単純群とする. $a\ (\neq 1) \in G$ とすれば, $\{1\} < \langle a \rangle \trianglelefteq G$. 従って, $\langle a \rangle = G$. 逆に, 素数位数の群は, 非自明な部分群を持たないので, 単純群である. □

補題 1.4.3 H を群 G の部分群とするとき, 次は同値である：

(1) $H \trianglelefteq G$,

(2) $xHx^{-1} = H, \quad \forall x \in G$,

(3) $xHx^{-1} \subset H, \quad \forall x \in G$.

証明　(1) $\Longleftrightarrow$ (2) $\Longrightarrow$ (3) は明らかである. (3) において, x を x^{-1} で置き換えると, $x^{-1}Hx \subset H\ (\forall x \in G)$. x, x^{-1} を左右からかけて, $H \subset xHx^{-1}\ (\forall x \in G)$ を得て, (3) と合わせて, (2) を得る. □

G を群とし, $x, y \in G$ とする. ある $z \in G$ が存在して,

$$x = zyz^{-1}$$

となるとき, x と y は **共役** であるという. 共役関係は群論において最も基本的な概念の一つである.

問 1.4.4 G を群とし, $x, y \in G$ とする. $x^y := yxy^{-1}$ とするとき, $(x^y)^{-1} = (x^{-1})^y$ を示せ. また, $z \in G$ のとき, $(x^y)^z = x^{zy}$ を示せ.

問 1.4.5 群 G における共役は, 同値関係であることを示せ. 即ち, x と y が共役のとき, $x \sim y$ と表すことにすると, 次が成り立つことを示せ:

(1) $x \sim x$ $(\forall x \in G)$,

(2) $x \sim y \implies y \sim x$,

(3) $x \sim y, y \sim z \implies x \sim z$.

例 1.4.2 $N \trianglelefteq G$ とする. $x \in N$ ならば, x に共役な元は, すべて N に含まれる.

H を群 G の部分群とし, $x \in G$ とする. G の部分群 xHx^{-1} を x に関する H の **共役部分群** という.

例 1.4.3 $N \leq G$ に対し, $N \trianglelefteq G$ であるための条件は, N の全ての共役部分群が N と一致することである.

例題 1.4.6 群 G の指数 2 の部分群 N は正規部分群であることを示せ.

（解） $a \in G$ を任意にとる. $a \in N$ ならば $aN = N = Na$. $a \notin N$ ならば $G = N + aN$ は左剰余類分解であり, $G = N + Na$ は右剰余類分解である. このとき

$$aN = G - N = Na.$$

従って $aN = Na$ $(\forall a \in G)$ が成り立ち, $N \triangleleft G$. □

例 1.4.4 S を群 G の部分集合とする. このとき

$$C_G(S) := \{a \in G \mid as = sa, \forall s \in S\}$$

は G の部分群をなす. $C_G(S)$ を S の **中心化群** という. 特に $C_G(G)$ を G の **中心** といい, $Z(G)$ と表す. $Z(G)$ は G の正規部分群である.

問 1.4.7 $C_G(S) \leq G$, $Z(G) \trianglelefteq G$ を証明せよ.

問 1.4.8 $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$ を示せ.

例 1.4.5 S を群 G の部分集合とする. このとき

$$N_G(S) := \{a \in G \mid aS = Sa\}$$

は G の部分群をなす. $N_G(S)$ を S の **正規化群** という. H が G の部分群のとき H は $N_G(H)$ の正規部分群である.

問 1.4.9 $N_G(S) \leq G$, $H \trianglelefteq N_G(H)$ を証明せよ. また, $H \trianglelefteq K \leq G$ ならば, $K \leq N_G(H)$ を確かめよ.

補題 1.4.10 H, K を群 G の部分群とするとき, 次が成り立つ.

(1) $H \trianglelefteq G \quad \Longrightarrow \quad HK \leq G.$

(2) $H \trianglelefteq G, K \trianglelefteq G \quad \Longrightarrow \quad HK \trianglelefteq G, \quad H \cap K \trianglelefteq G.$

証明　(1) $HK = KH$ が成り立つので, 補題 1.3.8 により, 結論を得る.
(2) $HK \leq G$, $H \cap K \leq G$ はよい. 任意の　$x \in G$ に対し, $H \trianglelefteq G$, $K \trianglelefteq G$ より, $xHK = HxK = HKx$, $x(H \cap K) = (H \cap K)x$. 従って, 結論を得る. □

対称群の正規部分群を決定しよう.

例 1.4.6 3 次対称群 S_3 において

$$\langle (1\ 2) \rangle \not\trianglelefteq S_3, \quad A_3 \trianglelefteq S_3.$$

例題 1.4.11 4 次対称群 S_4 の正規部分群は

$$\{1\}, \quad V_4, \quad A_4, \quad S_4$$

の 4 個であることを示せ.

（解）　$A_4 \trianglelefteq S_4$ はよい. V_4 は単位元と 3 個の $(2,2)$ 型の置換からなる. よって, 例 1.2.7 より, $V_4 \trianglelefteq S_4$. 逆に $N \trianglelefteq S_4$ とする. N が奇置換を含むとする. N が互換 τ を含めば, 任意の互換は, τ と共役でであり, $N = S_4$. N が長さ 4 の巡回置換を含むとする. $N \trianglelefteq S_4$ なので, N は長さ 4 の巡回置換すべて含む.

$$(1\ 3\ 2\ 4)(1\ 2\ 3\ 4)(2\ 1\ 3\ 4) = (2\ 4)$$

なので, N は互換を含み, $N = S_4$. 次に, N が奇置換を含まないとする, 即ち, $N \leq A_4$ とする. N が長さ 3 の巡回置換を含めば, 命題 1.3.14 (3) より, $N = A_4$. $N < A_4$ のとき, N が $(2,2)$ 型を含めば, $V_4 \leq N$. $|A_4 : V_4| = 3$ なので, $N = V_4$. □

例題 1.4.12 $N\ (\neq \{1\})$ を S_n の正規部分群とする. $n \neq 4$ ならば, $A_n \leq N$ であることを示せ.

（解）　$1 \leq n \leq 3$ の場合はよい. $n \geq 5$ とする. $\sigma\ (\neq 1) \in N$ に対し, $\sigma(i) \neq i$ となる i が存在する. $i \neq j \neq \sigma(i)$ なる j を選び, $\tau = (i\ j)$ とする. すると $\tau\sigma\tau^{-1}(j) = \sigma^{\tau}(j) = \sigma(i) \neq \sigma(j)$ なので, $\sigma^{\tau} \neq \sigma$, すなわち $\sigma\tau \neq \tau\sigma$.

$$[\sigma, \tau] := \sigma\tau\sigma^{-1}\tau^{-1} \ \in N$$

であり, 互いに異なる二つの互換 $\sigma\tau\sigma^{-1}$, τ の積である. 従って, $[\sigma, \tau]$ は, 長さ 3 の巡回置換であるか, $(2,2)$ 型である. 同じ型の元は互いに共役なので, 長さ 3 の巡回置換はすべて N に含まれるか, $(2,2)$ 型の元がすべて N に含まれる. 補題 1.3.14 により, $A_n \leq N$. □

1.4.2　剰余群

N を群 G の正規部分群とする. 二つの剰余類 aN, bN に対し, $Nb = bN$ なので, 集合 $aNbN = abN$ は剰余類である.

定理 1.4.13 N を群 G の正規部分群とする. 剰余類の積を $(aN)(bN) = (ab)N$ と定めると, G/N は群をなす. 単位元は N であり, aN の逆元は $a^{-1}N$ である. G が可換群ならば G/N も可換群である. また $|G/N| = |G : N|$.

証明 $((aN)(bN))cN = ((ab)N)cN = ((ab)c)N = (a(bc))N = aN((bc)N) = aN((bN)(cN))$ と結合法則が成り立つ. $N(aN) = aN = (aN)N$ となり, N は単位元である. また, $(a^{-1}N)(aN) = N = (aN)(a^{-1}N)$ が成り立ち, $(aN)^{-1} = a^{-1}N$. 以上により, (G1), (G2), (G3) が確かめられ, G/N は群をなす. G が可換群ならば $(aN)(bN) = abN = baN = (bN)(aN)$ が成り立ち, G/N も可換群である. □

例 1.4.7 S_4 の正規部分群 V_4 による剰余群の元を次のように表す：

$$S_4/V_4 = \{a_1 = V_4, a_2 = (1\ 2)V_4, a_3 = (1\ 3)V_4, a_4 = (2\ 3)V_4, a_5 = (1\ 2\ 3)V_4, a_6 = (1\ 3\ 2)V_4\}.$$

このとき, S_4/V_4 の乗積表は, 次の通りである：

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_6	a_5	a_4	a_3
a_3	a_3	a_5	a_1	a_6	a_2	a_4
a_4	a_4	a_6	a_5	a_1	a_3	a_2
a_5	a_5	a_3	a_4	a_2	a_6	a_1
a_6	a_6	a_4	a_2	a_3	a_1	a_5

S_3 の乗積表（例 1.2.4）と比べ,

$$a_1 \leftrightarrow 1,\ a_2 \leftrightarrow (1\ 2),\ a_3 \leftrightarrow (1\ 3),\ a_4 \leftrightarrow (2\ 3), a_5 \leftrightarrow (1\ 2\ 3),\ a_6 \leftrightarrow (1\ 3\ 2)\}$$

と対応させると, 群として, S_4/V_4 と S_3 が同じものと見なされる.

例 1.4.8 $N \trianglelefteq G$ とする. $N \leq H \leq G$ のとき $N \trianglelefteq H$ であり, H/N は G/N の部分群とみなせる. 例えば

$$A_4/V_4 = \{a_1, a_5, a_6\} \leq S_4/V_4 = \{a_1, a_2, a_3, a_4, a_5, a_6\}.$$

例 1.4.9 巡回群の剰余群は巡回群である. 実際, $G = \langle a \rangle$ ならば, $N \trianglelefteq G$ に対し, $G/N = \langle aN \rangle$ となる.

例 1.4.10 m を自然数とし, (m) を m の倍数全体のなす $\mathbb{Z}^+$ の部分群とする. このとき, $\mathbb{Z}/(m)$ は $[1] = 1 + (m)$ の生成する位数 m の巡回群である.

問 1.4.14 m を自然数とする. 加法群 $\mathbb{Z}/(m)$ の二元, 即ち, 二つの剰余類 $[a]$, $[b]$ に対し, 剰余類 $[ab]$ は, 代表元 a, b の取り方に依らず定まる. 従って, $[a] \cdot [b] = [ab]$ とすることにより, 積が定義される. このとき次を示せ.

(1) $(\mathbb{Z}/(m); \cdot)$ は単位可換半群をなす.

(2) $[a]$ が積に関し逆元を持つ為の必要十分条件は $(a,m)=1$, 即ち, a と m が互いに素となることである. このとき $[a]$ を **既約剰余類** という.

(3) 積に関し逆元を持つ全体 $(\mathbb{Z}/(m))^\times$ は, 位数 $\phi(m)$ の可換群をなす.

$(\mathbb{Z}/(m))^\times$ を, m を法とする, **既約剰余類群** という.

補題 1.4.15 N を群 G の正規部分群とし, $N \leq Z(G)$ とする. G/N が巡回群ならば, G はアーベル群である.

証明 G/N は巡回群なので, $G/N = \langle \bar{h} \rangle$ $(\bar{h} = hN)$ と表される. 任意の $g, g' \in G$ に対し, $\bar{g}(= gN) = \bar{h}^i, \bar{g'} = \bar{h}^{i'}$ $(\exists i, i')$ と表される. すると $g = h^i n, g' = h^{i'} n'$ $(\exists n, n' \in N)$ と表される. $n, n' \in N \subseteq Z(G)$ なので,

$$gg' = h^i n h^{i'} n' = h^{i+i'} nn' = h^{i'} n' h^i n = g'g.$$

従って G はアーベル群となる. □

1.5 群射と同型定理

1.5.1 群射の定義と基本的性質

群 $(G;\cdot)$ と群 $(G';*)$ に対し, 写像 $f : G \longrightarrow G'$ が

(GH) $f(a \cdot b) = f(a) * f(b) \quad (\forall a, b \in G)$

を満たすとき, f を G から G' への**群射** または **群準同型写像** という. 集合の写像として全射（単射）である群射を, **群全射**（**群単射**）という. 更に, 集合の写像として, 全単射である群射を, **群同型射** または **同型射** という. 同型射の逆写像も同型射である. G から G' への同型射が存在するとき G と G' は **同型**であるといい

$$G \simeq G'$$

と表す. G と G' が同形とは, 見かけは違っていても群としては同じものだという事である.

補題 1.5.1 $f : G \longrightarrow G'$ を群 G から G' への群射とするとき, 次が成り立つ.

(1) $f(1_G) = 1_{G'}$,

(2) $f(a^{-1}) = f(a)^{-1} \quad (\forall a \in G)$.

但し, $1_G, 1_{G'}$ は, G, G' の単位元である.

証明 (1) $1_G = 1_G \cdot 1_G$ なので $f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G)$, $f(1_G)^{-1}$ を両辺にかけて $1_{G'} = f(1_G)$ を得る.
(2) $1 = aa^{-1}$ に f を作用させて

$$1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}).$$

両辺に $f(a)^{-1}$ をかけて $f(a)^{-1} = f(a^{-1})$ を得る. □

例 1.5.1

$$f : \mathbb{C}^\times \longrightarrow \mathrm{GL}_n(\mathbb{C}), \quad \alpha \longmapsto \alpha I_n$$

は群単射である.

例 1.5.2

$$\det : \mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathbb{C}^\times, \quad A \mapsto \det(A)$$

は群全射である.

例 1.5.3 正の実数のなす乗法群を $\mathbb{R}^\times_{>0}$ と表すとき,

$$\log : \mathbb{R}^\times_{>0} \longrightarrow \mathbb{R}^+, \quad x \mapsto \log x$$

は同型射であり, その逆写像は

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times_{>0}, \times), \quad x \mapsto e^x$$

である.

問 1.5.2

$$f : G \longrightarrow G', \quad g : G' \longrightarrow G''$$

が共に群射ならば, 合成射 $g \circ f : G \longrightarrow G''$ も群射であることを示せ.

問 1.5.3 $f : G \longrightarrow G'$ が群同型射ならば, f^{-1} も群同型射であることを示せ.

例 1.5.4 $H \leq G$ のとき,

$$\iota : H \longrightarrow G, \quad h \longmapsto h$$

は群単射である. これを **自然な群単射** という.

例 1.5.5 N を群 G の正規部分群とする. 写像

$$\pi : G \longrightarrow G/N, \quad a \longmapsto aN$$

は群全射であり, **自然な群全射** と呼ばれる.

例 1.5.6 $G_1, \cdots, G_n$ を群とし, $G_1 \times \cdots \times G_n$ をその直積とする. 各 i に対し写像

$$pr_i : G_1 \times G_2 \times \cdots \times G_n \longrightarrow G_i, \ (a_1, a_2, \cdots, a_n) \longmapsto a_i$$

は, 群全射であり, i 番目への **射影** と呼ばれる. また写像

$$\iota_i : G_i \longrightarrow G_1 \times G_2 \times \cdots \times G_n, \ a_i \mapsto (1, \cdots, 1, a_i, 1, \cdots, 1)$$

は, 群単射であり, i 番目の **埋め込み** と呼ばれる. この埋め込みにより, 時に, G_i を, $\iota_i(G_i)$ と同一視して, $G_1 \times G_2 \times \cdots \times G_n$ の部分群と見なす.

問 1.5.4 $f : G \longrightarrow G'$ を群全射とする. G が可換群ならば, G' も可換群であることを示せ.

定義より, 次を得る：

補題 1.5.5 $f : G \longrightarrow G'$ を群射とする. このとき次が成り立つ.

(1) $H \leq G \quad \Longrightarrow \quad f(H) \leq G'$,

(2) $H' \leq G' \quad \Longrightarrow \quad f^{-1}(H') \leq G$,

(3) $H' \trianglelefteq G' \quad \Longrightarrow \quad f^{-1}(H') \trianglelefteq G$,

(4) f が群全射のとき, $N \trianglelefteq G \quad \Longrightarrow \quad f(N) \trianglelefteq G'$.

問 1.5.6 補題 1.5.5 を証明せよ.

$f : G \longrightarrow G'$ を群射とするとき, G の正規部分群 $f^{-1}(1)$ を, f の **核** といい, $\mathrm{Ker}(f)$ と表す.

補題 1.5.7 $f : G \longrightarrow G'$ を群射とするとき,

$$\mathrm{Ker}(f) = \{1\} \quad \Longleftrightarrow \quad f \text{ は単射.}$$

証明 $(\Rightarrow)$ $f(a) = f(b)$ ならば $1 = f(a)f(b)^{-1} = f(ab^{-1})$, 故に $ab^{-1} \in \mathrm{Ker}(f) = \{1\}$ となり $a = b$ を得る, よって f は単射である. $(\Leftarrow)$ $a \in \mathrm{Ker}(f)$ とすると, $f(a) = 1 = f(1)$. f は単射なので $a = 1$ を得て, $\mathrm{Ker}(f) = \{1\}$. □

例 1.5.7 群 G から自分自身への同形射を, 特に **自己同形射** という. G の自己同形射の全体 $\mathrm{Aut}(G)$ は写像の合成を積として群をなす. $\mathrm{Aut}(G)$ を群 G の **自己同形群** という.

問 1.5.8 $C_m = \langle a \rangle$ を位数 m の巡回群とする. このとき, $\mathrm{Aut}(C_m) \simeq (\mathbb{Z}/(m))^\times$ を証明せよ.

例 1.5.8 G を群とし, $a \in G$ とする.

$$\sigma_a : G \longrightarrow G, \quad b \longmapsto b^a = aba^{-1}$$

を a の定める **内部自己同型射** という. 内部同型射の全体を $\mathrm{Inn}(G)$ と表すと, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ が成り立つ. $\mathrm{Inn}(G)$ を G の **内部自己同型群** といい, $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ を **外部自己同型群**という.

群射の有限個, または無限個の列

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} \cdots \longrightarrow G_{i+1} \xrightarrow{f_{i+1}} \cdots$$

は

$$\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \quad (\forall i)$$

を満たすとき **完全列** と呼ばれる. 完全列

$$1 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 1$$

を **短完全列** という. このとき G を G' の G'' による **拡大** ともいう. ここで, 1 は自明な群 $\{1\}$ を表す.

問 1.5.9 次を証明せよ.

(1) $1 \longrightarrow G' \xrightarrow{f} G$ が完全列 $\iff$ f が単射,

(2) $G \xrightarrow{g} G'' \longrightarrow 1$ が完全列 $\iff$ g が全射.

例 1.5.9

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{C}) \xrightarrow{f} \mathrm{GL}_n(\mathbb{C}) \xrightarrow{g} \mathbb{C}^\times \longrightarrow 1$$

は短完全列である. ここで f は自然な群単射, g は行列式を取る写像：$g(A) = \det(A)$.

問 1.5.10 $f : G \longrightarrow G'$ を群射とするとき,

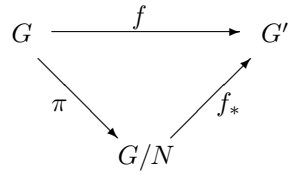
$$1 \longrightarrow \mathrm{Ker}(f) \xrightarrow{\iota} G \xrightarrow{f} \mathrm{Im}(f) \longrightarrow 1$$

は, 群の短完全列であることを確かめよ. 但し, ι は自然な群単射であり, $f : G \longrightarrow \mathrm{Im}(f)$ は f の値域を $\mathrm{Im}(f)$ に取り換えた群射である.

1.5.2 群射の分解定理

次の定理は, 任意の群射が, 自然な群全射と群単射の合成写像であることを主張する.

定理 1.5.11 （群射の分解定理）$f : G \longrightarrow G'$ を群射とし, $N := \mathrm{Ker}(f)$ とする. このとき, 群単射 $f_* : G/N \longrightarrow G'$ が存在し, $f = f_* \circ \pi$ を満たす：



ただし $\pi : G \longrightarrow G/N$ は自然な群全射である.

証明 $f_*(aH) := f(a)$ は, 剰余類 aH の代表元 a の取り方によらず定まる. 何故ならば, $aH = bH$ とすると $b^{-1}a \in H \leq N$ なので, $1 = f(b^{-1}a) = f(b^{-1})f(a) = f(b)^{-1}f(a)$ となり, $f_*(aH) = f(a) = f(b) = f_*(bH)$ を得る. よって, 写像 $f_* : G/H \longrightarrow G'$ が定義される. このように定義された f_* は

$$f_* \circ \pi(a) = f_*(aH) = f(a), \quad \forall a \in G$$

となるので $f_* \circ \pi = f$ を満たし, $\mathrm{Im}(f_*) = \mathrm{Im}(f)$. 更に

$$f_*(aHbH) = f_*(abH) = f(ab) = f(a)f(b) = f_*(aH)f_*(bH)$$

を満たすので群射である. $H = N$ のとき, $f_*(aN) = f_*(bN)$ とすると, f_* の定義より $f(a) = f(b)$. よって, $b^{-1}a \in \mathrm{Ker}(f) = N$ となり $aN = Nb$ を得て, f_* が単射であることがわかる. □

系 1.5.12（第 1 同型定理）$f : G \longrightarrow G'$ を群全射とする．$N' \trianglelefteq G'$ ならば $N := f^{-1}(N') \trianglelefteq G$ であり $G/N \simeq G'/N'$. 特に, $G/\mathrm{Ker}(f) \simeq G'$.

証明　補題 1.5.5 (3) より, $N \trianglelefteq G$. $\pi : G' \longrightarrow G'/N'$ を自然な群全射とすると, 合成写像 $g := \pi \circ f : G \longrightarrow G'/N'$ は群全射である．このとき $\mathrm{Ker}(g) = g^{-1}(1) = f^{-1}(\pi^{-1}(1)) = f^{-1}(N') = N$ が成り立ち, 定理より, $G/N \simeq G'/N'$. □

例題 1.5.13 G を群とし, 部分群 $N \leq K \leq G$ は共に G の正規部分群とする．このとき, $K/N \trianglelefteq G/N$ であり,

$$G/K \simeq (G/N)/(K/N)$$

であることを証明せよ.

（解）　最初の主張は明らかである．自然な群全射 $p : G \longrightarrow G/N, q : G/N \longrightarrow (G/N)/(K/N)$ の合成写像を π とすると, その核は K に等しい．従って, 系 1.5.12 より, $G/K \simeq (G/N)/(K/N)$. □

例 1.5.10 $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ は群全射であり, $\mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{C})$ なので

$$\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) \simeq \mathbb{C}^\times.$$

例題 1.5.14 $C = \langle a \rangle$ を a で生成された巡回群とする, このとき次が成り立つことを示せ.

$$C \quad \simeq \quad \begin{cases} \mathbb{Z} & |C| = \infty \text{ のとき,} \\ \mathbb{Z}/(n) & |C| = n < \infty \text{ のとき.} \end{cases}$$

（解）　写像

$$f : \mathbb{Z} \longrightarrow C, \quad m \longmapsto a^m$$

は全射であり, 補題 1.1.11 により, 群射である．補題 1.3.17 により, $|C| = n < \infty$ のとき, $\mathrm{Ker}(f) = (n)$. 系 1.5.12 により $C \simeq \mathbb{Z}/(n)$. 一方 $|C| = \infty$ のとき, 例 1.3.14 より, f は単射であることがわかる．従って f は同型射である. □

例 1.5.11 例 1.4.7 を再確認しよう．4 次の対称群 S_4 において, V_4 の単位元以外の元を

$$\mathbf{1} = (1\ 4)(2\ 3), \quad \mathbf{2} = (1\ 3)(2\ 4), \quad \mathbf{3} = (1\ 2)(3\ 4)$$

とおく. 写像

$$f : S_4 \longrightarrow S_3 \simeq S(\{\mathbf{1}, \mathbf{2}, \mathbf{3}\})$$

を

$$\sigma \longmapsto \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1}^\sigma & \mathbf{2}^\sigma & \mathbf{3}^\sigma \end{pmatrix}, \quad \mathbf{i}^\sigma = \sigma \mathbf{i} \sigma^{-1}$$

により定めると, f は群射となる．このとき $\mathrm{Ker}(f) = V_4$ となり, f が全射であることもわかる．従って, 同型定理により

$$S_4/V_4 \simeq S_3.$$

定理 1.5.15 （第 2 同型定理）N を群 G の正規部分群、H を G の部分群とするとき

$$HN/N \simeq H/H \cap N.$$

証明 $HN = NH$ は G の部分群である. 写像

$$f : H \longrightarrow HN/N, \qquad h \mapsto hN$$

は $f(hh') = hh'N = hNh'N = f(h)f(h')$ をみたすので, 群射である. HN/N の任意の元は $hnN = hN$ と表されるので, f は全射である. 一方 $\mathrm{Ker}(f) = H \cap N$ なので, 同型定理 1.5.12 より結論を得る. □

例題 1.5.16 G を群 H をその部分群とする. このとき次を示せ.

(1) H の正規化群 $N_G(H)$ の元 a に対し

$$\sigma_a : H \longrightarrow H, \quad h \mapsto aha^{-1}$$

は自己同型射である.

(2)

$$\sigma : N_G(H) \longrightarrow \mathrm{Aut}(H), \quad a \mapsto \sigma_a$$

は群射である.

(3) $\mathrm{Ker}(\sigma)$ は H の中心化群 $C_G(H)$ に等しい.

(4) $N_G(H)/C_G(H)$ は $\mathrm{Aut}(H)$ の部分群に同型である.

（解） (1) $H \triangleleft N_G(H)$ なので, $aha^{-1} \in H$ である. また, σ_a は群同型射である（例 1.5.8 参照）.
(2) $\sigma_{ab}(h) = (ab)h(ab)^{-1} = a(bhb^{-1})a^{-1} = \sigma_a(\sigma_b(h)) = (\sigma_a \circ \sigma_b)(h)$ が任意の $h \in H$ に対し成り立つ. 従って $\sigma_{ab} = \sigma_a \circ \sigma_b$ となり, σ は群射である.
(3) $a \in \mathrm{Ker}(\sigma)$ ならば, $\sigma_a(h) = aha^{-1} = h$ $(\forall h \in H)$. 従って, $a \in C_G(H)$. 逆も同様.
(4). 定理 1.5.11 より直ちに得られる. □

定理 1.5.17 （対応定理）N を群 G の正規部分群とし, $\pi : G \longrightarrow G/N$ を自然な群全射とする. N を含む G の部分群全体の集合を $\mathcal{S}$, G/N の部分群全体の集合を $\mathcal{T}$ と表す：

$$\mathcal{S} = \{H \leq G \mid N \leq H \leq G\}; \quad \mathcal{T} = \{\bar{H} \mid \bar{H} \leq G/N\}.$$

写像

$$\Phi : \mathcal{S} \longrightarrow \mathcal{T}, \quad H \mapsto H/N = \pi(H), \quad \Psi : \mathcal{T} \longrightarrow \mathcal{S}, \quad \bar{H} \mapsto \pi^{-1}(\bar{H})$$

は互いに逆写像である. 特に, これらは全単射である.
更に, $H_1, H_2 \in \mathcal{S}$ に対し,

$$H_1 \trianglelefteq H_2 \quad \Longleftrightarrow \quad H_1/N \trianglelefteq H_2/N.$$

証明 $N \leq H \leq G$ とすると, $\pi^{-1}(\pi(H)) = H$ が成り立つ. また, $\bar{H} \leq G/N$ とすると, $N \leq \pi^{-1}(\bar{H}) \leq G$ であり, π は全射なので,

$$\pi(\pi^{-1}(\bar{H})) = \bar{H}.$$

従って, $\Psi \circ \Phi = I_{\mathcal{S}}, \Phi \circ \Psi = I_{\mathcal{T}}$.

$h \in H_2$ に対し, 次が成り立つ：

$$hH_1h^{-1} \subset H_1 \quad \Longleftrightarrow \quad \bar{h}\bar{H}_1\bar{h}^{-1} \subset \bar{H}_1.$$

従って, 最後の主張を得る. □

例 1.5.12 $\mathbb{Z}$ の部分群 $12\mathbb{Z}$ を含む部分群は $\{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}\}$ の 6 個であり, それぞれ $G = \mathbb{Z}/12\mathbb{Z}$ の部分群

$$G = \mathbb{Z}/12\mathbb{Z},\ 2\mathbb{Z}/12\mathbb{Z},\ 4\mathbb{Z}/12\mathbb{Z},\ 6\mathbb{Z}/12\mathbb{Z},\ 12\mathbb{Z}/12\mathbb{Z} = \{0\}$$

に対応する.

例 1.5.13 例 1.5.11 で確かめたように $S_4/V_4 \simeq S_3$. 3 次の対称群 S_3 の部分群は

$$\{1\}, \quad \langle(1\ 2)\rangle, \quad \langle(1\ 3)\rangle, \quad \langle(2\ 3)\rangle, \quad A_3 = \langle(1\ 2\ 3)\rangle, \quad S_3$$

の 6 個である. これらの部分群に対応する V_4 を含む S_4 の部分群は

$$V_4,\ \langle(1\ 4\ 2\ 3),\ (1\ 2)\rangle,\ \langle(1\ 2\ 3\ 4), (1\ 3)\rangle,\ \langle(1\ 3\ 4\ 2), (2\ 3)\rangle,\ A_4,\ S_4$$

の 6 個である.

例 1.5.14 $m, n \in \mathbb{Z}$ に対し, 群射

$$f : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}, \quad (x, y) \longmapsto (mx, ny)$$

を考える. $mn \neq 0$ ならば, $\mathrm{Ker}(f) = \{0\} \oplus \{0\} = \{0\}$, $\mathrm{Im}(f) = (m) \oplus (n)$ であり,

$$0 \longrightarrow \mathrm{Im}(f) \xrightarrow{\iota} \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\pi} \mathbb{Z} \oplus \mathbb{Z}/\mathrm{Im}(f) \longrightarrow 0$$

は, 短完全列である. ただし ι, π は, 自然な群単射である. 更に次の同形を得る：

$$\mathbb{Z} \oplus \mathbb{Z}/\mathrm{Im}(f) = (\mathbb{Z} \oplus \mathbb{Z})/((m) \oplus (n)) \simeq \mathbb{Z}/(m) \oplus \mathbb{Z}/(n).$$

従って $|\mathbb{Z} \oplus \mathbb{Z}/\mathrm{Im}(f)| = |mn|$.

定理 1.5.18 $H_1, \cdots, H_n$ を群 G の部分群とする, 写像

$$f : H_1 \times \cdots \times H_n \longrightarrow G, \quad f(h_1, \cdots, h_n) = h_1 \cdots h_n$$

が同型射であるためには, つぎの (1),(2),(3) が成り立つことが必要かつ十分条件である.

(1) $i, j(i \neq j)$ に対し, H_i の元と H_j の元は交換可能.

(2) $G = H_1 \cdots H_n$.

(3) 任意の i に対し $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}$.

証明 f は同型射とする. ι_i, ι_j を i, j 番目の埋め込みとすると, $a \in H_i, b \in H_j$ に対し

$$f(ab) = f(\iota_a))f(\iota_b) = f(\iota_i(a)\iota_j(b)) = f(\iota_j(b)\iota_j(a)) = f(\iota_j(b))f(\iota_i(a)) = f(ba).$$

f は同型射なので, $ab = ba$ を得る. f は同型射なので, 全射であり (2) を得る.
(3) $h_i = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ とすると, f は同型射なので,

$$(1, \cdots, 1, h_i, 1, \cdots, 1) = (h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_n)$$

となり, $h_1 = \cdots = h_n = 1$.
逆に, (1),(2),(3) が成り立つとする.

$$f(h_1, \cdots, h_n)(h'_1, \cdots, h_n)) = f(h_1 h'_1, \cdots, h_n h'_n) = h_1 h'_1 \cdots h_n h'_n$$

であり, (1) より, $h_1 h'_1 \cdots, h_n h'_n = (h_1 \cdots h_n)(h'_1 \cdots h'_n)$ が成り立つので, f は群射であることがわかる. また, (2) より, f が全射であることがわかる. $(h_1, \cdots, h_n) \in \mathrm{Ker}(f)$ とすれば,

$$h_1^{-1} = h_2 \cdots h_n \in H_1 \cap H_2 \cdots H_n.$$

従って, (3) より, $h_1 = 1 = h_2 \cdots h_n$ を得る. これを繰り返し, $h_1 = h_2 = \cdots = h_n = 1$ を得て, $\ker(f) = \{1\}$ を得る. よって, f は単射となり, 同型射である. □

定理の条件を満たすとき, G は部分群 $H_1, \cdots, H_n$ の（内部）**直積** といい

$$G = H_1 \times \cdots \times H_n$$

と表す.

注意 1.5.1 G がアーベル群, 特に加法群の場合, G を部分群 $H_1, \cdots, H_n$ の**直和** といい,

$$G = H_1 \oplus \cdots \oplus H_n$$

と表す.

補題 1.5.19 H, K を群 G の正規部分群とし, 補題 1.5.18 の (2),(3) を満たすならば, G は部分群 H, K の直積である.

証明 $h \in H, k \in K$ に対し, $[h, k] = hkh^{-1}k^{-1} \in H \cap K = \{1\}$. 従って, $hk = kh$ が成り立ち, 補題 1.5.18 (1) を満たし, $G = H \times K$ となる. □

補題 1.5.20 $H, K \trianglelefteq G$ に対し,

$$(|H|, |K|) = 1 \quad \Longrightarrow \quad HK = H \times K.$$

証明 $|H| = n, |K| = m$ とする. $x \in H \cap K$ とすると, $x^m = 1 = x^n$. 従って, $|x| = 1$ となり, $H \cap K = 1$. 従って, 補題 1.5.19 より, $HK = H \times K$. □

例 1.5.15 実数のなす乗法群 $\mathbb{R}^\times$ は, 正の実数のなす部分群 $\mathbb{R}^\times_{>0}$ と, 位数 2 の部分群 $\mu_2 = \{1, -1\}$ との直積である：

$$\mathbb{R}^\times = \mathbb{R}^\times_{>0} \times \{1, -1\}.$$

例 1.5.16 複素数のなす乗法群 $\mathbb{C}^\times$ は, 正の実数のなす乗法群 $\mathbb{R}^\times_{>0}$ と, 絶対値 1 の複素数のなす部分群 $\mathbb{C}^\times_1$ との直積である：

$$\mathbb{C}^\times = \mathbb{R}^\times_{>0} \times \mathbb{C}^\times_1.$$

1.6 群作用

1.6.1 群作用と置換表現

G を群とし, X を空でない集合とする. 写像

$$G \times X \longrightarrow X, \quad (g, x) \mapsto gx$$

は, 次を満たすとき G の X への（左からの）**作用** と呼ばれる.

(GA1) $(gh)x = g(hx), \quad g, h \in G,\ x \in X.$

(GA2) $1x = x, \quad x \in X.$

このとき G を X の **変換群**, X を G**-集合** という.

G が集合 X に作用するとき, $g \in G$ に対し

$$\pi(g) : X \longrightarrow X, \quad \pi(g)(x) = gx$$

と定める. すると, $\pi(g) \in \mathrm{Sym}(X)$ であり, 写像

$$\pi_\sigma : G \longrightarrow \mathrm{Sym}(X), \quad g \longmapsto \pi(g) \tag{1.6}$$

は群射である. π_σ を, 作用 σ に付随する, G の X における **置換表現** という.

逆に, 群射 $\pi : G \longrightarrow \mathrm{Sym}(X)$ が与えられたとき, 写像

$$\sigma_\pi : G \times X \longrightarrow X; \quad (g, x) \longmapsto \pi(g)(x)$$

は, G の X への作用である.

このようにして, G の X への作用 σ と, G の X に於ける置換表現 π_σ は $1:1$ に対応する.

問 1.6.1 作用 σ に置換表現 π_σ を対応させる写像は全単射であることを確かめよ.

例 1.6.1 n 次の対称群 S_n は集合 $X = \{1, 2, \cdots, n\}$ に

$$S_n \times X \longrightarrow X, \quad (\sigma, i) \longmapsto \sigma(i)$$

により作用する.

群 G が集合 X に作用するとき, $x \in X$ に対し

$$G_x = \{g \in G \mid gx = x\}, \quad G \cdot x = \{gx \mid g \in G\}$$

は, それぞれ G の部分群, X の部分集合であり, x に於ける **安定化部分群**, x の **軌道** と呼ばれる.

次は, 定義から得られる.

補題 1.6.2 群 G が集合 X に作用しているとする. このとき

$$x \sim y \quad \Longleftrightarrow \quad G \cdot x = G \cdot y$$

と定義すると, $\sim$ は同値関係であり, x を含む同値類は x の軌道 $G \cdot x$ に一致する.

例 1.6.2 F を体とし, 群として $\mathrm{GL}_n(F)$, 集合として $\mathrm{M}_n(F)$ をとる. このとき

$$\mathrm{GL}_n(F) \times \mathrm{M}_n(F) \longrightarrow \mathrm{M}_n(F); \quad (P, M) \longmapsto PMP^{-1}$$

は作用である. M, N が同じ軌道に含まれる必要かつ十分条件は M と N が相似であることである：

$$\exists P \in \mathrm{GL}_n(F) \quad \text{s.t.} \quad M = PNP^{-1}.$$

補題 1.6.3 群 G が集合 X に作用しているとする. このとき $x \in X$ に対し

$$|G \cdot x| = |G : G_x|.$$

証明 $G_x = H$ と置く. $gH = hH$ とするとき $gx = hx$. 従って, 写像

$$\phi : G/H \longrightarrow G \cdot x, \quad \phi(gH) = gx$$

を定めることが出来る. また $gx = \phi(gH) = \phi(g'H) = g'x$ ならば $g^{-1}g' \in H$ となり, $gH = g'H$. 従って ϕ は単射である. 全射は明らかなので与式を得る. □

次の定理は, 同値関係による分割である.

定理 1.6.4 （軌道分解定理）群 G が集合 X に作用しているとする. 相異なる軌道の全体を $\{G \cdot x_i\}_{i \in I}$ と表すと

$$X = \sum_{i \in I} G \cdot x_i.$$

特に X が有限集合のとき,

$$|X| = \sum_{i \in I} |G \cdot x_i| = \sum_{i \in I} |G : G_{x_i}|.$$

群 G が集合 X に作用しているとする. X の元からなる, 長さ m の任意の 2 列

$$(x_1, \cdots, x_n),\ (y_1, \cdots, y_n), \quad x_1, \cdots, x_n(\neq),\ y_1, \cdots, y_n(\neq)$$

に対し

$$(gx_1, \cdots, gx_n) = (y_1, \cdots, y_n), \quad \exists g \in G$$

のとき, G は X 上 n 重 **可移** という. 一重可移のとき, 単に, **可移** という.

例 1.6.3 S_n は, 集合 $X = \{1, \cdots, n\}$ 上 n 重可移であり, A_n は X 上 $n-2$ 重可移である.

例 1.6.4 G が X 上可移のとき, $X = G \cdot x$ $(\forall x \in X)$ であり, $|X| = |G : G_x|$.

G を群とする. G の演算

$$G \times G \longrightarrow G, \quad (g, x) \mapsto gx$$

を G の自分自身への作用と見ることが出来る. このとき, (1.6) において定義された群射

$$\pi : G \longrightarrow \mathrm{Sym}(G), \quad g \longmapsto \pi_g$$

は単射でり. G の **正則表現** と呼ばれる.

従って次の定理を得る：

定理 1.6.5 （Cayley）位数 n の群 G は, n 次対称群 S_n の部分群と同型である.

例 1.6.5 （剰余類）H を群 G の部分群とする. G の演算を制限した写像

$$H \times G \longrightarrow G, \quad (h, x) \mapsto hx$$

は H の G への作用である. このとき $x \in G$ の軌道は $H \cdot x = Hx$ であり, x を含む右剰余類に他ならない. さらに軌道分解は群 G の H に関する右剰余類分解に他ならない.

例 1.6.6 （両側剰余類）H, K を群 G の二つの部分群とする. 写像

$$(H \times K) \times G \longrightarrow G, \quad ((h, k), x) \longmapsto hxk^{-1}$$

は直積 $H \times K$ の G への作用である. このとき $x \in G$ の軌道 $(H \times K) \cdot x = HxK$ を, x を含む (H, K) **両側剰余類** という. 相異なる両側剰余類の全体を $\{Hx_iK \mid i \in I\}$ とおくとき, 軌道分解

$$G = \sum_{i \in I} Hx_iK$$

を群 G の (H, K) **両側剰余類分解** という.

補題 1.6.6 H, K を有限群 G の二つの部分群とし, $a \in G$ とする. 両側剰余類 HaK に含まれる H に関する右剰余類の集合を $\mathcal{R}$ とする：

$$\mathcal{R} = \{Hak \mid k \in K\}.$$

このとき,

$$|\mathcal{R}| = |K : a^{-1}Ha \cap K|, \quad |HaK| = |H||K : a^{-1}Ha \cap K|.$$

特に,

$$|HK| = |H||K|/|H \cap K|.$$

証明 写像

$$K \times \mathcal{R} \longrightarrow \mathcal{R}, \quad (k, Ha) \longmapsto Hak^{-1}$$

は K の $\mathcal{R}$ への作用である. このとき, K は $\mathcal{R}$ 上可移であり, $Ha \in \mathcal{R}$ における安定化部分群は $K_{Ha} = a^{-1}Ha \cap K$ となる. よって, 補題 1.6.4 により

$$|\mathcal{R}| = |K : a^{-1}Ha \cap K|.$$

従って, $|HaK| = |H||\mathcal{R}| = |H||K : a^{-1}Ha \cap K|$. $a = 1$ とすれば, 最後の主張を得る. □

1.6.2 共役作用

G の G 自身への作用

$$G \times G \longrightarrow G, \quad (g,h) \mapsto ghg^{-1}$$

を **共役作用** という. 共役作用は, 群論において, とりわけ重要である.

共役作用が定める G 上の同値関係 $''\sim''$ は, 次のように定義される:

$$h_1 \sim h_2 \quad \Longleftrightarrow \quad gh_1g^{-1} = h_2 \ (\exists g \in G).$$

このとき h_1 と h_2 は共役であるといった. h における安定化部分群

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\}$$

は h の中心化群 $C_G(h)$ である. また h の軌道

$$G \cdot h = \{ghg^{-1} \mid g \in G\}$$

を h を含む **共役類** といい, $\mathrm{Conj}(h)$ と表す.

例 1.6.7 N を群 G の正規部分群とする. このとき, N はいくつかの共役類の和集合である.

共役作用に対応する置換表現

$$G \longrightarrow \mathrm{Sym}(G), \quad g \mapsto (h \mapsto ghg^{-1})$$

の核は群 G の中心 $Z(G) = \{g \in G \mid gh = hg, \forall h \in G\}$ である.

定義より,

$$h \in Z(G) \quad \Longleftrightarrow \quad \mathrm{Conj}(h) = \{h\}.$$

が成り立つので, 軌道分解定理（定理 1.6.4) より, 次を得る：

定理 1.6.7 （類等式）有限群 G に対し, その中心を $Z(G) = \{z_1 = 1, z_2, \cdots, z_r\}$ とする. G の相異なる共役類を $C_1 = \{z_1\}, \cdots, C_r = \{z_r\}, C_{r+1} = \mathrm{Conj}(g_{r+1}), \cdots, C_{r+s} = \mathrm{Conj}(g_{r+s})$ とするとき

$$G = C_1 + \cdots + C_{r+s}$$

であり

$$|G| = |Z(G)| + |G : C_G(g_{r+1})| + \cdots + |G : C_G(g_{r+s})|.$$

例 1.6.8 S_4 に含まれる置換の型は $(1,1,1,1), (2,1,1), (2,2), (3,1), (4)$ であり, これらの型を持つ置換として,

$$\sigma_1 = 1, \ \sigma_2 = (1\ 2), \ \sigma_3 = (1\ 2)(3\ 4), \ \sigma_4 = (1\ 2\ 3), \ \sigma_5 = (1\ 2\ 3\ 4)$$

をとる. これらを含む共役類は,

$$\begin{array}{rcl} C(\sigma_1) & = & \{1\} \\ C(\sigma_2) & = & \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\} \\ C(\sigma_3) & = & \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \\ C(\sigma_4) & = & \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2,4,3)\}, \\ C(\sigma_5) & = & \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\} \end{array} .$$

従って, S_4 の類等式は $24 = 1 + 6 + 3 + 8 + 6$ である.

位数 が素数 p の冪（べき）である群を p 群という.

補題 1.6.8 $Z(G)$ を p 群 G の中心とする. このとき $|Z(G)| = p^a$ $(\exists a \geq 1)$.

証明　前定理の記号をそのまま用いる. 類等式の左辺は p の冪であり, 右辺の $|G : C_G(g_{r+i})|$ $(1 \leq i \leq s)$ は, $g_{r+i} \notin Z(G)$ なので G の位数の真の約数となり, p で割れる. 従って $|Z(G)|$ も p で割れる. □

補題 1.6.9 G を非可換 p 群とすると p^2 は $|G : Z(G)|$ を割り切る.

証明　G は p 群なので $|G : Z(G)|$ は p の冪である. G は非可換なので $|G : Z(G)| \neq p^0 = 1$. もし $|G : Z(G)| = p$ とすれば, $G/Z(G)$ は位数 p の巡回群. 従って 補題 1.4.15 により, G はアーベル群となり, 矛盾である. よって, p^2 は $|G : Z(G)|$ の約数である. □

例題 1.6.10 p を素数とするとき, 位数 p^2 の群 G は, 次のいずれかであることを示せ：

(1) 位数 p^2 の巡回群.

(2) 位数 p の巡回群の二つの直積.

（解）　先ず G がアーベル群であることを示す. G は p 群なのでその中心 $Z(G)$ の位数は p 以上である. 従って $|G : Z(G)|$ は 1 または p. 従って上の例から非可換では有り得ない.

位数 p^2 の元 g を含めば, $G = \langle g \rangle$ となり G は巡回群となる. G が位数 p^2 の元を含まないとする. 単位元と異なる $g \in G$ の位数は p である. また $h \in G \backslash \langle g \rangle$ をとると, $\langle g \rangle \cap \langle h \rangle = \{1\}$. 写像

$$f : \langle g \rangle \times \langle h \rangle \longrightarrow G, \quad (g^i, h^j) \mapsto g^i h^j$$

は準同型写像である. $(g^i, h^j) \in \mathrm{Ker}(f)$ ならば, $g^i h^j = 1$. $g^i = (h^j)^{-1} \in \langle g \rangle \cap \langle h \rangle = \{1\}$. 従って $g^i = h^j = 1$ となり, $\mathrm{Ker}(f) = \{1\}$. よって f は単射, 位数を比べて全射となる. □

例 1.6.9 G を群とし, G の部分集合全体の集合, 即ち, G の冪集合を $\mathcal{P}(G)$ と表す. このとき写像

$$G \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G), \quad (g, U) \mapsto gUg^{-1}$$

は G の $\mathcal{P}(G)$ への作用である. この作用に対し $S \in \mathcal{P}(G)$ に於ける安定化部分群は S の正規化群である：

$$G_S = N_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

$S, T \in \mathcal{P}(G)$ は, $T = gSg^{-1}$ となる $g \in G$ が存在するとき, **共役** であるという. 従って S の軌道は S と共役な部分集合の集まりであり, その個数は, 補題 1.6.3 により $|G : N_G(S)|$ である.

1.6.3 Sylow の定理

この節では, 有限群論で最も基本的な定理である Sylow の定理を証明する.

補題 1.6.11 p 群 G が有限集合 X に作用しているとし,

$$\mathrm{Fix}(G) = \{x \in X \mid G \cdot x = \{x\}\}$$

とする. このとき,

$$|X| \equiv |\mathrm{Fix}(G)| \pmod{p}.$$

証明 X を軌道分解する:

$$X = \mathrm{Fix}(G) + \sum_{i=1}^{n} G \cdot x_i$$

ここで, $G \cdot x_1, \cdots, G \cdot x_n$ は位数が 1 より大きい軌道である. $|G \cdot x_i| = |G : G_{x_i}| = p^{e_i}$ $(e_i \geq 1)$ が成り立つ. 従って, 補題の式を得る. □

G を位数 n の有限群とし, $n = p_1^{e_1} \cdots p_r^{e_r}$ を素因数分解とする. このとき, 位数 $p_i^{e_i}$ の部分群を **Sylow p_i 部分群** という.

例 1.6.10 S_4 の Sylow 2-部分群は, 位数 8 で,

$$\langle (1\ 2\ 3\ 4), (1\ 3) \rangle,\ \langle (1\ 2\ 4\ 3), (1\ 4) \rangle,\ \langle (1\ 3\ 2\ 4), (1\ 2) \rangle$$

の 3 個ある. Sylow 3-部分群は, 位数は 3 で,

$$\langle (1\ 2\ 3) \rangle,\quad \langle (1\ 2\ 4) \rangle,\quad \langle (1\ 3\ 4) \rangle,\quad \langle (2\ 3\ 4) \rangle$$

の 4 個である.

定理 1.6.12 $p^a \big|| G|$ ならば, G は位数 p^a の部分群を持つ. 特に Sylow p 部分群は存在する.

証明 $G = p^b m,\ (p, m) = 1$ とする.

$$X := \{S \subset G \,\big|\, |S| = p^a\}$$

とすると,

$$|X| = \binom{p^b m}{p^a} = \frac{p^b m (p^b m - 1) \cdots (p^b m - p^a + 1)}{p^a (p^a - 1) \cdots 2 \cdot 1}.$$

$b \geq a$ なので,

$$\mathrm{ord}_p(p^b m - i) = \mathrm{ord}_p(p^a - i) \quad (1 \leq i \leq p^a - 1).$$

従って, $p^{b-a} \big|| X|$, $p^{b-a+1} \nmid |X|$. G は, $S \longmapsto gS$ により, X に作用する. そこで, X を軌道分解する:

$$X = O_1 + \cdots + O_n.$$

このとき, $p^{b-a+1} \nmid |O_i|$ を満たす軌道が存在する. $O_i = G \cdot S_i$ とすると, $O_i \simeq G/G_{S_i}$. 従って, $p^a \big|| G_{S_i}|$ でなければならない.

一方, $s \in S_i$ を固定するとき,

$$G_{S_i} \longrightarrow S_i; \quad g \longmapsto gs$$

は単射なので, $|G_{S_i}| \leq |S_i| = p^a$. よって, G_{S_i} は位数 p^a の部分群である. □

定理 1.6.13 (Sylow の定理) G を位数 n の有限群とし, p を n の素因数とする. このとき次が成立つ.

(1) 任意の p 部分群はある Sylow p 部分群に含まれる.

(2) Sylow p 部分群は互いに共役である.

(3) Sylow p 部分群の個数は $|G : N_G(S)|$ に等しく, $kp+1$ の形である. ここで S は Sylow p 部分群である.

証明 (1) P を任意の p 部分群とし, S を Sylow p 部分群 とする. P は S の左剰余類の集合 G/S に作用する. そこで,

$$G/S = \sum_{i=1}^{l} P \cdot g_i S$$

を軌道分解とする. $|P \cdot gS| = |P/P_{gS}|$ は p 冪であるが, $|G/S|$ は p と素である. 従って, 或る $P \cdot g_i S$ は 1 点集合である. 即ち,

$$xg_iS = g_iS \quad (\forall x \in P)$$

となり, $g_i^{-1} P g_i \leq S$. 即ち, $P \leq g_i S g_i^{-1}$. (2) は (1) に於いて P として Sylow p 部分群をとればよい.
(3) 群 G は Sylow p 部分群の集合に, 共役により, 可移に作用する. S を Sylow p 部分群とすると, Sylow p 部分群の個数は $|G \cdot S| = |G : \mathrm{N}_G(S)|$ に等しい.

さて, Sylow p 部分群 S は, G/S に作用する.

$$\mathrm{Fix}(S) = \{gS \mid xgS = gS \ (\forall x \in S)\}$$

とすると, 補題 1.6.11 により,

$$|\mathrm{Fix}(S)| \equiv |G/S| \pmod{p}.$$

$|G/S|$ は p と素なので, $|\mathrm{Fix}(S)|$ も p と素である. $gS \in \mathrm{Fix}(S)$ となる為の条件は, $S = gSg^{-1}$. 即ち, $g \in \mathrm{N}_G(S)$. 従って, $\mathrm{Fix}(S) \simeq \mathrm{N}_G(S)/S$.

$$|G/\mathrm{N}_G(S)| = |G : S|/|\mathrm{N}_G(S) : S| = r$$

とすると, 補題 1.6.11

$$r|\mathrm{Fix}(S)| = r|\mathrm{N}_G(S) : S| = |G : S| \equiv |\mathrm{Fix}(S)| \pmod{p}.$$

従って, $(p, |\mathrm{Fix}(S)|) = 1$ なので, $r \equiv 1 \pmod{p}$. □

例題 1.6.14 $1 \leq q < p$ を二つの素数とし G を位数 pq の群とする. このとき, Sylow p 部分群 P は G の正規部分群であることを示せ.

（解） P の正規化群を $N(P)$ とすると

$$P \leq N(P) \leq G.$$

$|G : P| = q$ は素数なので, $N(P) = P$ であるか, $N(P) = G$ となる. $P = N(P)$ とすると P と共役な部分群の個数 $|G : N(P)|$ は, $|G : N(P)| = |G : P| = q$ に等しい. $2 \leq q < p$ より $q \not\equiv 1 \pmod{p}$ となり, 定理の (3) に反する. 故に $N(P) = G$ となり $P \trianglelefteq G$ である. □

例題 1.6.15 群 G の位数が 6 のとき, $G \simeq C_2 \times C_3 \simeq C_6$ であるか, $G \simeq S_3$ であることを示せ. ここで C_i は位数 i の巡回群を表す.

（解） Sylow 3-群を P, Sylow 2-群を Q とおく. P, Q は位数が $3, 2$ の群であり, その生成元を a, b とする：

$$P = \langle a \rangle, \quad Q = \langle b \rangle.$$

例題 1.6.14 により, $P \triangleleft G$. 従って $b^{-1}ab \in P$. $b^{-1}ab = a$ のとき $G \simeq P \times Q$. このとき, $G = \langle ab \rangle$ は, 位数 6 の巡回群である.

また $b^{-1}ab = a^2 = a^{-1}$ のとき

$$f : S_3 \longrightarrow G, \quad \tau^i\sigma^j \longmapsto b^i a^j$$

は同型写像である. ただし $\tau = (1\ 2), \quad \sigma = (1\ 2\ 3)$. □

例題 1.6.16 群 G の位数が 15 ならば $G \simeq C_3 \times C_5 \simeq C_{15}$.

証明 Sylow 3 群の個数は $3k + 1$ と表され, 15 の約数なので, $k = 0$. また Sylow 5 群の個数は $5k + 1$ で 15 の約数なので $k = 0$. 従って Sylow 3-群 N, Sylow 5 群-K は共に正規部分群である.

$$[n, k] = nkn^{-1}k^{-1} \in N \cap K = \{1\}, \quad n \in N, k \in K$$

なので, 写像

$$f : N \times K \longrightarrow G, \quad (n, k) \longmapsto nk$$

は群単射である. $|N \times K| = |G| = 15$ なので, 全射でもあり, f は群同型射である. $N \simeq C_3, K \simeq C_5$ であるので, $G \simeq C_3 \times C_5$. 最後の部分は明らかであろう. □

補題 1.6.17 P を有限群 G の Sylow p 部分群とし, N を G の正規部分群とする. このとき次が成り立つ.

(1) PN/N は G/N の Sylow p 部分群である.

(2) $P \cap N$ は N の Sylow p 部分群である.

証明　(1) 第二同型定理により

$$PN/N \simeq P/P \cap N.$$

従って PN/N は p 群である. $|G/N : PN/N| = |G : PN|$ は, $|G : P|$ の約数なので p と素. 従って PN/N は G/N の Sylow p 部分群である.
(2)　$N \cap P$ は p 群であり,

$$|PN : P| = |PN : N \cap P|/|P/N \cap P| = |PN : N \cap P|/|PN/N| = |N : N \cap P|$$

は $|G : P|$ の約数なので p と素. 従って $P \cap N$ は N の Sylow p 部分群である. □

補題 1.6.18　（Frattini 論法）H を有限群 G の正規部分群とし, P を H の Sylow p 部分群とすれば, $G = N_G(P)H$ である.

証明　$H \trianglelefteq G$ なので, 任意の $x \in G$ に対し,

$$x^{-1}Px \subset x^{-1}Hx = H.$$

位数を考えれば, $x^{-1}Px$ も H の Sylow p 部分群である. Sylow の定理により,

$$x^{-1}Px = h^{-1}Ph, \quad \exists h \in H.$$

従って $(xh^{-1})^{-1}Pxh^{-1}h = P$ となり, $xh^{-1} \in N_G(P)$. 従って, $x \in N_G(P)H$ となる. □

1.6.4　半直積

この節では, これまで 群 G の集合 X への作用を考察した. この小節では, 群 G の群 N への作用を考察する.

写像

$$\sigma : G \times N \longrightarrow N; \quad (g, n) \longmapsto g \cdot n$$

は, 次を満たすとき, 群 G の群 N への作用と呼ばれる：

(1) 任意の g に対し, $\sigma_g : n \longmapsto g \cdot n$ は N の自己同型射である.

(2) $(gg') \cdot n = g \cdot (g \cdot n) \quad (\forall g, g' \in G, \forall n \in N)$.

即ち,

$$\pi : G \longrightarrow \mathrm{Aut}(N); \quad g \longmapsto \sigma_g$$

は群射である. π を, 作用 σ に付随する, G の, N の自己同型群としての, **表現** という.

群 G が群 N に作用するとする. このとき, 直積集合 $N \times G$ の二元 $(n, g), (n', g')$ に対し,

$$(n, g)(n', g') = (n(g \cdot n), gg')$$

と定めると, $N \times G$ は群をなす. この群を N と G との **半直積** といい, $N : G$ と表す.

問 1.6.19　次を示せ.

(1) $G \times G$ は群をなし, $(n,g)^{-1} = (g^{-1} \cdot n^{-1}, a^{-1})$.

(2) $\iota : G \longrightarrow N \times G,\ g \longmapsto (1,g),\ N \longrightarrow N \times G,\ n \longmapsto (n,1)$ は共に群単射である.

(3) 上の単射により, N, G を $N \times G$ の部分群と見なす. このとき, $N \trianglelefteq N \times G$ であり,

$$N \cap G = \{1\}, \quad N \times G = NG.$$

一般に, $N \trianglelefteq L$ とする. $G \leq L$ が

$$N \cap G = \{1\}, \quad L = NG$$

を満たすとき, N を G の（L に於ける）**補群** という.

補題 1.6.20 群の拡大

$$1 \longrightarrow N \xrightarrow{f} L \xrightarrow{g} G \longrightarrow 1 \tag{1.7}$$

に於いて, 次は同値である：

(1) 群射 $h : G \longrightarrow L$ が存在して $g \circ h = I_G$ を満たす.

(2) $\mathrm{Im}(f) \simeq N$ は補群を持つ.

この条件が満たされるとき, 拡大 (1.7) は **分裂する** という.

問 1.6.21 上の補題を証明せよ.

定理 1.6.22 $N \trianglelefteq L$ とし, G を N の補群とする. すると, G は共役により, N に作用し, この作用による半直積を $N : G$ と表す. このとき,

$$\phi :\ N : G \longrightarrow L; \quad (n,g) \longmapsto ng$$

は同型射である.

証明 ϕ は, 次の様に, 群射である：

$$\begin{aligned} \phi((n,g)(n',g')) &= \phi(n(gn'g^{-1}), gg') \\ &= n(gn'g^{-1})gg' = ngn'g' \\ &= \phi(n,g)\phi(n',g'). \end{aligned}$$

また, G が G の補群であることより, ϕ が単射であり全射である. □

例 1.6.11 G を群とする. $a \in G$ に対し, $a_L \in \mathrm{Sym}(G)$ を

$$a_L : G \longrightarrow G; \quad g \longmapsto ag$$

とする. このとき, $G_L = \{a_L \mid a \in G\}$ は $\mathrm{Sym}(G)$ の正規部分群をなす. $\mathrm{Aut}(G)$ は G_L に作用する：

$$\alpha \cdot a_L = (\alpha\ a)_L \quad (\alpha \in \mathrm{Aut}(G)).$$

このとき, $G_L : \mathrm{Aut}(G) \simeq G_L : \mathrm{Aut}(G)$ を G のホロモルフという.

例 1.6.12 $G = \langle a \rangle$ を位数 n の巡回群とし, $G = \langle b \rangle$ を位数 2 の群とする.

$$b \cdot a = a^{-1}$$

とすると, G は G に作用する. このとき, $D_{2n} \simeq G : G$. 但し, D_{2n} は位数 $2n$ の二面体群である.

1.7　正規列

1.7.1　作用域をもつ群

Λ を集合とし, G を群とする. 写像

$$\sigma : \Lambda \times G \longrightarrow G; \quad (\lambda, a) \longmapsto \lambda a$$

が与えられ

$$\lambda\, ab = (\lambda a)(\lambda b) \qquad (\forall a, b \in G)$$

を満たすとき, G を **作用域 Λ をもつ群**, 或は **Λ-群** という.

Λ-群 G の自己準同型のなす集合を $\mathrm{End}(G)$ と表すとき,

$$\phi_\lambda : G \longrightarrow G; \quad a \longmapsto \lambda a$$

は G の自己準同型射となり, 写像

$$\phi : \Lambda \longrightarrow \mathrm{End}(G); \quad \lambda \longmapsto \phi_\lambda$$

を得る. 逆に, 写像 $\phi : \Lambda \longrightarrow \mathrm{End}(G)$ が与えられれば, $\sigma(\lambda, a) = \phi_\lambda(a)$ とすることにより, G は Λ-群の構造をもつ.

Λ-群 G の（正規）部分群 H は,

$$\lambda \in \Lambda,\ h \in H \quad \Longrightarrow \quad \lambda h \in H$$

を満たすとき, **Λ-（正規）部分群** と呼ばれる. Λ の各元は H の自己準同型を導くので, H 自身が Λ-群である. G と $\{1\}$ は Λ-正規部分群であるが, これら以外に Λ-正規部分群を持たないとき, G は **Λ-既約**, または **Λ-単純** であるという.

Lambda-正規部分群 N に対し,

$$aN = bN \quad \Longrightarrow \quad (\lambda a)N = (\lambda b)N$$

が成り立つ. 従って, 剰余群 G/N に対し, 作用

$$\Lambda \times G/N \longrightarrow G/N \quad (\lambda, aN) \longmapsto (\lambda a)N$$

が定まり, G/N は Λ-群となる. Λ-群の間の群射 $f : G \longrightarrow G'$ が Λ の作用と可換なとき, 即ち,

$$f(\lambda a) = \lambda f(a) \quad (\lambda \in \Lambda,\ a \in G)$$

が成り立つとき, f を **Λ-準同型写像**, または **Λ-群射** という. Λ-同型などの定義もこれに準ずる.

$\Lambda = \emptyset$ とすれば, Λ-群, Λ-部分群, Λ-群射は, 通常の群, 部分群, 群射に他ならない. Λ-群の研究は, 群の研究を含んでいる.

例 1.7.1 G を群とし, $\mathrm{Inn}(G)$ を作用域とするとき, $\mathrm{Inn}(G)$-部分群は正規部分群である. また, $\mathrm{Aut}(G)$ を作用域とするとき, $\mathrm{Aut}(G)$-部分群を **特性部分群** という.

定理 1.7.1 （Λ-群射の分解定理）$f : G \longrightarrow G'$ を Λ-群射とし, $N := \mathrm{Ker}(f)$ とする. このとき, 次が成り立つ：

(1) $\mathrm{Im}(f)$ は G' の Λ-部分群である.

(2) N は Λ-正規部分群である.

(3) Λ-群単射 $f_* : G/N \longrightarrow G'$ が存在し, $f = f_* \circ \pi$ を満たす：

$$\begin{array}{ccc} & f & \\ G & \longrightarrow & G' \\ \pi \searrow & & \nearrow f_* \\ & G/N. & \end{array}$$

ただし $\pi : G \longrightarrow G/N$ は自然な群全射である.

問 1.7.2 Λ-群射に対する第 1 , 第 2 同型定理及び対応定理を, 群射の場合を参考に, 記述し証明せよ.

1.7.2 正規列と組成列

Λ-群 G に於ける Λ-部分群列

$$(\mathcal{C}) \quad G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_r = \{1\}$$

は

$$G_i \trianglerighteq G_{i+1}, \quad i = 0, 1, \cdots r-1$$

を満たすとき, 長さ r の **Λ-正規列** と呼ばれ, r 個の剰余群の成す列

$$\{G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r = G_{r-1}\}$$

を, Λ-正規列 $(\mathcal{C})$ の **Λ-剰余群列** という. Λ-部分群 $\{G_i\}$ には同じものがあっても良いことに注意する.

例 1.7.2 $\Lambda = \emptyset$ とする. 4 次の対称群 S_4 の部分群列

$$(\mathcal{S}) \quad S_4 \geq A_4 \geq V_4 \geq \{1\}$$

は長さ 3 の正規列であり, その剰余群列は

$$\{S_4/A_4, A_4/V_4, V_4/\{1\} = V_4\}.$$

Λ-群 G の二つの Λ-正規列

$$(\mathcal{C}_1)\quad G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{1\},$$

$$(\mathcal{C}_2)\quad G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_s = \{1\}$$

に対し,

$$G = H_0 = G_0, H_1 = G_{i_1}, \cdots, H_j = G_{i_j}, \cdots, H_s = G_r = 1$$

となる $0, 1, \cdots, r$ の部分列 $0, i_1, \cdots, i_j, \cdots, r = i_s$ が存在するとき, $(\mathcal{C}_1)$ は $(\mathcal{C}_2)$ の **細分** という.

例 1.7.3 $\Lambda = \emptyset$ とする. S_4 の正規列

$$(\mathcal{T})\quad S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq \langle(12)(34)\rangle \trianglerighteq \{1\}$$

は, 例 1.7.2 の正規列 $(\mathcal{S})$ の細分である.

Λ-正規列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{1\}$$

は, 真の細分を持たないとき, **Λ-組成列** と呼ばれる. Λ-組成列の剰余群列を特に **Λ-組成剰余群列** という.

Λ-組成列は, $\Lambda = \emptyset$ のとき, 単に **組成列** と呼ばれ, $\Lambda = \mathrm{Inn}(G)$ のとき, **主組成列**, $\Lambda = \mathrm{Aut}(G)$ のとき, **特性組成列** と呼ばれる.

例 1.7.4 例 1.7.3 の $(\mathcal{T})$ は組成列であり, その組成剰余群列は

$$S_4/A_4 \simeq C_2,\ A_4/V_4 \simeq C_3,\ V_4/\langle(12)(34)\rangle \simeq C_2,\ \langle(12)(34)\rangle \simeq C_2$$

である. ここで C_n は位数 n の巡回群である.

N を Λ-群 G の Λ-正規部分群とする.

$$N \lneqq M \lneqq G$$

となる Λ-正規部分群 M が存在しないとき, N を G の **極大 Λ-正規部分群** という.

定義より, 次を得る:

補題 1.7.3 Λ-群 G の Λ-正規列

$$(\mathcal{C})\quad G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{1\}$$

が Λ-組成列である為の必要十分条件は, 各 $i = 0, 1, \cdots, r-1$ に対して, G_{i+1} が G_i の極大 Λ-正規部分群であることである.

補題 1.7.3 と対応定理 1.5.17 より, 次を得る:

命題 1.7.4 Λ-組成剰余群列を構成する群は Λ-単純群である.

問 1.7.5 有限群は組成列をもつことを確かめよ.

1.7.3 Schreier の細分定理と Jordan-Hölder の定理

補題 1.7.6 (Zassenhaus の補題) G を Λ-群とし, H_1, H_2, K_1, K_2 をその Λ-部分群とし

$$H_2 \trianglelefteq H_1, \quad K_2 \trianglelefteq K_1$$

とする. このとき, 次が成り立つ：

$$H_2(H_1 \cap K_1)/H_2(H_1 \cap K_2) \simeq (H_1 \cap K_1)K_2/(H_2 \cap K_1)K_2.$$

証明 (1) $H_2 \triangleleft H_1$ なので, 第 2 同型定理より,

$$H_1(H_1 \cap K_1)/H_1 \simeq H_1 \cap K_1/H_2 \cap K_1.$$

この同型により, $H_2(H_1 \cap K_2)/H_1$ と $/(H_1 \cap K_2)(H_2 \cap K_1)/H_2 \cap K_1$ が対応し,

$$H_2(H_1 \cap K_1)/H_2(H_1 \cap K_2) \simeq H_1 \cap K_1/(H_1 \cap K_2)(H_2 \cap K_1)$$

を得る. H と K の役割を交換して,

$$K_2(K_1 \cap H_1)/K_2(K_1 \cap H_2) \simeq H_1 \cap K_1/(H_1 \cap K_2)(H_2 \cap K_1).$$

従って,

$$H_2(H_1 \cap K_1)/H_2(H_1 \cap K_2) \simeq K_2(K_1 \cap H_1)/K_2(K_1 \cap H_2)$$

を得る. □

定理 1.7.7 (Schreier の細分定理) Λ-群 G の二つの Λ-正規列

$$(\mathcal{C}_1) \quad G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_r = \{1\},$$

$$(\mathcal{C}_2) \quad G = K_0 \trianglerighteq K_1 \trianglerighteq K_2 \trianglerighteq \cdots \trianglerighteq K_s = \{1\}$$

が与えられたとき, 次の性質を満たす $(\mathcal{C}_1), (\mathcal{C}_2)$ の細分 $(\mathcal{C}_1'), (\mathcal{C}_2')$ が存在する.

$(\mathcal{C}_1'), (\mathcal{C}_2')$ は, 長さが等しく, それらの Λ-剰余群列を適当に並べ替えると, 対応する剰余群が同型になる.

証明 $H_i \geq H_{i+1}$ の間に部分群列

$$H_i = H_{i,0} \geq H_{i,1} \geq \cdots \geq H_{i,s} = H_{i+1}, \quad H_{i,j} = (H_i \cap K_j)H_{i+1}$$

を挿入し, $K_j \geq K_{j+1}$ の間に部分群列

$$K_j = K_{j,0} \geq K_{j,1} \geq \cdots \geq K_{j,r} = K_{j+1}, \quad K_{j,i} = (K_j \cap H_i)K_{j+1}$$

を挿入する. すると

$$(\mathcal{C}_1') \quad G = H_{0,0} \geq H_{0,1} \geq \cdots \geq H_{0,s} = H_1 = H_{1,0} \geq H_{1,1} \geq \cdots \geq H_{r,1} \geq \cdots \geq H_{r,s} = \{1\},$$

$$(\mathcal{C}_2') \quad G = K_{0,0} \geq K_{0,1} \geq \cdots \geq K_{0,r} = K_1 = K_{1,0} \geq K_{1,1} \geq \cdots \geq K_{s,1} \geq \cdots \geq K_{s,r} = \{1\}$$

は, それぞれ $(\mathcal{C}_1), (\mathcal{C}_2)$ の長さ rs の細分である. また, Zassenhaus の補題により

$$\begin{aligned} H_{i,j}/H_{i,j+1} &= (H_i \cap K_j)H_{i+1}/(H_i \cap K_{j+1})H_{i+1} \\ &\simeq (K_j \cap H_i)K_{j+1}/(K_j \cap H_{i+1})K_{j+1} = K_{j,i}/K_{j+1,i}. \end{aligned}$$

従って $(\mathcal{C}_1'), (\mathcal{C}_2')$ は求めるものである. □

定理 1.7.8 （Jordan-Hölder の定理）Λ-群 G は Λ-組成列を持つと仮定する. $(\mathcal{C}_1), (\mathcal{C}_2)$ が G の Λ-組成列ならば, これらの長さは等しく, Λ-組成剰余群は適当に並べ替えると, それぞれ, 同型になる.

証明

$$(\mathcal{C}_1) \quad G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_r = \{1\},$$

$$(\mathcal{C}_2) \quad G = K_0 \trianglerighteq K_1 \trianglerighteq K_2 \trianglerighteq \cdots \trianglerighteq K_s = \{1\}$$

とする. Schreier の細分定理における, これらの細分 $(\mathcal{C}_1'), (\mathcal{C}_2')$ を作る. このとき, これらの剰余群列は順序を無視すれば一致する. 剰余群が単位群になるときを調べよう. 細分の仕方は, 次の通りであった：

$$H_i = H_{i,0} \geq H_{i,1} \geq \cdots \geq H_{i,s} = H_{i+1}, \quad H_{i,j} = (H_i \cap K_j)H_{i+1}.$$

H_{i+1} は H_i の極大正規部分群なので,

$$H_i = H_{i,0} = \cdots = H_{i,j} > H_{i,j+1} = \cdots = H_{i,s} = H_{i+1}, \quad \exists j.$$

従って, 剰余群が単位群とならないものは $(\mathcal{C}_1')$ では

$$H_0/H_1, \cdots, H_{r-1}/H_r = H_{r-1}$$

の r 個である. 同様にして $(\mathcal{C}_2')$ の剰余群列のうち, 単位群とならないものは

$$K_0/K_1, \cdots, K_{s-1}/K_s = K_{s-1}$$

の s 個である. $(\mathcal{C}_1')$ と $(\mathcal{C}_2')$ の剰余群列は一致するのだから, $r = s$ であり, これら r 個の群は順序を適当に取れば, 互いに同型である. □

1.7.4 交換子群と可解群

G を群とし, $x, y \in G$ とする. G の元 $[x, y] := xyx^{-1}y^{-1}$ を x, y の交換子という. $X, Y \leq G$ に対し,

$$[X, Y] = \langle [x, y] \mid x, y \in G \rangle$$

と定める.

補題 1.7.9 G を群とする. $a, b, c \in G$, $X, Y \leq G$ に対し, 次が成り立つ：

(1) $[a,b]=1 \iff ab=ba$.

(2) $[a,b]^{-1}=[b,a]$.

(3) $[X,Y]=1 \iff xy=yx\ (\forall x\in X, \forall y\in Y)$.

(4) $f:G\longrightarrow H$ を群射とするとき, $f([a,b])=[f(a),f(b)]$, $f([X,Y])=[f(X),f(Y)]$.

(5) $[ab,c]=a[b,c]a^{-1}[a,c], [a,bc]=[a,b]b[a,c]b^{-1}$.

(6) $X\leq N_G(Y) \iff [X,Y]\leq Y$.

(7) $[X,Y]=[Y,X]\trianglelefteq\langle X,Y\rangle$.

問 1.7.10 上の補題を証明せよ.

$G^{(1)}=[G,G]$ を群 G の **交換子群** という. $n>1$ に対し, $G^{(n)}=[G^{(n-1)},G^{(n-1)}]$ と定義し, $G^{(0)}=G$ とする.

補題 1.7.11 G を群とし, $H\leq G$ とするとき, 次が成り立つ:

(1) $H^{(n)}\leq G^{(n)}$.

(2) $f:G\longrightarrow K$ を群全射とするとき, $f(G^{(n)})=K^{(n)}$.

(3)

$$G^{(1)}\leq H \iff H\trianglelefteq G,\ G/H:\text{可換群}.$$

証明 ($\Longrightarrow$) $h\in H, g\in G$ に対し, $[h,g]\in G^{(1)}\leq H$. 従って, $ghg^{-1}g^{-1}\in H$ が成り立ち, $H\trianglelefteq G$. $\bar{g_1},\bar{g_2}\in G/H$ に対し,

$$[\bar{g_1},\bar{g_2}]=[g_1,g_2]H=H.$$

従って, G/H は可換群である. ($\Longleftarrow$) 任意の g_1,g_2 に対し, $[g_1,g_2]H=H$ となり, $G^{(1)}\leq H$. □

群 G の正規列

$$(\mathcal{C})\quad G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_n=\{1\}$$

において, 剰余群 G_{i-1}/G_i が全て可換群であるとき, $(\mathcal{C})$ を **可換正規列** という. 可換正規列を持つ群を **可解群** という.

例 1.7.5 アーベル群は可解群である.

例 1.7.6

$$S_3\trianglerighteq A_3\trianglerighteq\{1\}$$

は, 可換正規列であり, S_3 は可解群である. また

$$S_4\geq A_4\geq V_4\geq\{1\}$$

は, 可換正規列であり, S_4 は可解群である.

補題 1.7.12

$$G \text{ 可解群} \quad \Longleftrightarrow \quad G^{(n)} = \{1\} \ (\exists n \in \mathbb{N}).$$

証明　$G^{(n)} = 1$ ならば

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} = \{1\}$$

は可換正規列である. 逆に,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$$

を可換正規列とする. 帰納法により, $G^{(i)} \leq G_i$ を示そう. $i = 0$ のときは自明. i のとき正しいとする. 補題 1.7.11 (3) より, $[G_i, G_i] \leq G_{i+1}$. 従って, 帰納法の仮定により,

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_i, G_i] \leq G_{i+1}$$

を得る. □

問 1.7.13 非可換単純群は可解群ではないことを確かめよ.

定理 1.7.14 可解群の部分群は可解群である.

証明　H を可解群 G の部分群とする. 補題 1.7.11 (1) より, $H^{(n)} \leq G^{(n)} = \{1\}$ $(\exists n \in \mathbb{N})$ なので, H は可解群である. □

定理 1.7.15 N を 群 G の正規部分群とするとき, 次は同値である：

(1) G は可解群である.

(2) $N, G/N$ は共に可解群である.

証明　(1) $\Longrightarrow$ (2) 前定理により, N は可解群である. $\pi : G \longrightarrow G/N$ を自然な全射とするとき, 補題 1.7.11 (2) より, $\pi(G^{(n)}) = (G/N)^{(n)}$. 従って, G が可解なので, G/N も可解である.
(2) $\Longrightarrow$ (1) N の可換正規列を

$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_s = \{1\}$$

とし, G/N の可換正規列を

$$G/N = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_t = \{1\}$$

とする. 自然な群全射

$$\pi : G \longrightarrow G/N$$

による H_i の逆像を G_i とする. このとき, 対応定理 1.5.17 と例題 1.5.13 より

$$G_i \trianglerighteq G_{i+1}, \quad G_i/G_{i+1} \simeq H_i/H_{i+1}.$$

従って

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_t = N = N_0 \trianglerighteq \cdots \trianglerighteq N_s = \{1\}$$

は, 可換正規列である. よって G は可解群である. □

1.7.5 $A_n(n \geq 5)$ の単純性と $S_n(n \geq 5)$ の非可解性

補題 1.7.16 $n \geq 5$ とし, A_n の正規部分群 N は長さ 3 の巡回置換を含むとする. このとき, $N = A_n$.

証明 $\sigma = (a, b, c) \in N$ とし, $\sigma_1 = (i, j, k)$ を長さ 3 の任意の巡回置換とする. τ を

$$a \mapsto i, \quad b \mapsto j, \quad c \mapsto k$$

となる置換とする. $\tau \in A_n$ ならば, $\sigma_1 = \tau\sigma\tau^{-1} \in N$. τ が奇置換ならば, m, n を i, j, k と異なる文字とし, $\tau_1 = (m\ n)\tau$ とする. このとき, $\tau_1 \in A_n$ であり, $\tau_1\sigma\tau_1^{-1} = (m\ n)(i, j, k)(m\ n) = (i, j, k) \in N$. 従って, N は, 長さ 3 の巡回置換をすべて含む. 命題 1.3.14 (3) より, $N = A_n$. □

定理 1.7.17 $n \geq 5$ ならば A_n は単純群である.

証明 $N \neq \{1\}$ を A_n の正規部分群とし, $\sigma\ (\neq 1) \in N$ とする. 置換 σ の型を

$$(d_1, \cdots, d_r) \quad (d_1 \geq \cdots \geq d_r)$$

とする.
(1) $d_1 \geq 4$ の場合.

$$\sigma = (a_1\ a_2\ a_3\ \cdots\ a_k)(b_1\ b_2\ \cdots)\cdots$$

とすると,

$$[\sigma, (a_1\ a_2\ a_3)] = (a_1\ a_4\ a_2) \in N.$$

従って, 補題 1.7.16 より, $N = A_n$
(2) $d_1 = 3$, $d_2 \geq 2$ の場合.

$$\sigma = (a_1\ a_2\ a_3)(b_1\ b_2\ \cdots)\cdots$$

とすると,

$$[\sigma, (a_1\ a_2\ b_1)] = (a_1\ b_1\ a_3\ b_2\ a_2)$$

となり, (1) の場合となる.
(3) $d_1 = 3$, $d_2 = 1$ の場合はよい.
(4) $d_1 = d_2 = 2$ の場合.

$$\sigma = (a_1\ a_2)(b_1\ b_2)\cdots$$

とし, $c \notin \{a_1, a_2, b_1, b_2\}$ とする. $\sigma(c) = c$ ならば,

$$[\sigma, (a_1\ b_1\ c)] = (a_1\ a_2\ b_2\ c\ b_1) \in N$$

となり, (1) の場合となる. $\sigma(c) = c' \neq c$ ならば,

$$[\sigma, (a_1\ b_1\ c)] = (a_1\ c\ b_1)(a_2\ b_2\ c') \in N$$

となり, (2) の場合となる.

いずれの場合も, N は長さ 3 の巡回置換を含み, $N = A_n$ となり, A_n は非可換単純群である. □

次の定理は方程式論において重要である.

定理 1.7.18 $n \geq 5$ ならば S_n は可解群ではない.

証明 S_n が可解群とすれば, 定理 1.7.14 により, A_n も可解群である. しかし, 定理 1.7.17 により A_n は非可換単純群であるので, 可解群ではない. 従って, S_n は可解群ではない. □

1.7.6 特性部分群と冪零群

G を群とし, $H \leq G$ とする. H が特性部分群であるとき, 即ち, $\sigma(H) = H$ $(\forall \sigma \in \mathrm{Aut}(G))$ を満たすとき, H char G と表す.

例 1.7.7 群の中心は特性部分群である：$Z(G)$ char G.

例 1.7.8 G の極大部分群全体の共通部分を $\Phi(G)$ と表し, Frattini 部分群という. $\Phi(G)$ は G の特性部分群である：$\Phi(G)$ char G.

問 1.7.19 特性部分群は正規部分群であることを確かめよ.

補題 1.7.20 (1) H char K, K char $G \implies H$ char G.

(2) H char K, $K \triangleleft G \implies H \triangleleft G$.

(3) H char G, K char $G \implies HK$ char G, $H \cap K$ char G.

問 1.7.21 上の補題を証明せよ.

G を群とし,

$$L_1(G) = G, \quad L_n(G) = [L_{n-1}(G), G] \ (n > 1)$$

と定める. $L_n(G) = \{1\}$ $(\exists n \in \mathbb{N})$ となるとき, G を **冪零群** という. $m = \min\{i \mid L_i(G) = \{1\}\}$ とするとき, G を $m-1$ **級** の冪零群という.

補題 1.7.22 (1) $L_n(G)$ char G $(n \geq 1)$.

(2) $L_{n+1}(G) \leq L_n(G)$.

(3) $L_n(G)/L_{n+1}(G) \leq Z(G/L_{n+1}(G))$.

証明 (1) n に関する帰納法で示す. $\sigma \in \mathrm{Aut}(G)$ ならば, 補題 1.7.11 (3) より, $\sigma([G,G]) = [\sigma(G), \sigma(G) = [G,G]$. よって, $n = 1$ のときは正しい. n のときまで正しいとすると, $\sigma \in \mathrm{Aut}(G)$ ならば,

$$\sigma(L_{n+1}(G)) = \sigma([L_n(G), G]) = [L_n(G), G]$$

が成り立ち, $n+1$ の場合も正しい. (2) $L_n(G) \trianglelefteq G$ なので, 補題 1.7.11 (5) より, $L_{n+1}(G) = [L_n(G), G] \leq L_n(G)$ を得る. (3) $[L_n(G), G] = L_{n+1}(G)$ より結論を得る. □

$Z_0(G) = \{1\}$ とし, 次の様に, 帰納的に $Z_n(G)$ を定める：

$$Z_n(G) := \pi_{n-1}^{-1}(Z(G/Z_{n-1}(G)).$$

但し, $\pi_{n-1} : G \longrightarrow G/Z_{n-1}(G)$ は自然な全射である.

問 1.7.23 $Z_n(G)$ char G を示せ.

補題 1.7.24

$$G : \text{冪零群} \quad \Longleftrightarrow \quad G = Z_n(G)\ (\exists n \geq 0).$$

G が冪零群ならば, $k = \min\{n \mid G = Z_n(G)\}$ が G の級である.

証明 G が m 級の冪零群ならば, $L_{m+1-i}(G) \leq Z_i(G)$ $(0 \leq i \leq m)$ が成り立つことを示す. $i = 0$ のとき, $L_{m+1}(G) = 1 = Z_0(G)$. $i > 0$ とする. $L_{m+2-i}(G) \leq Z_{i-1}(G)$ とすると, $[L_{m+1-i}(G), G] = L_{m+2-i}(G) \leq Z_{i-1}(G)$. 従って,

$$L_{m+1-i}(G)Z_{i-1}(G)/Z_{i-1}(G) \leq Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G).$$

よって, $L_{m+1-i}(G) \leq Z_i(G)$. 従って, 帰納法により, 上の主張が得られた. 特に, $G = L_1(G) = Z_m(G)$ であり, $k \leq m$.

逆に, $Z_n(G) = G$ $(\exists n \geq 0)$ が成り立つとする. このとき, $L_{i+1}(G) \leq Z_{n-i}(G)$ $(0 \leq i \leq n)$ が成り立つことを示す. $i = 0$ のときは明らかに成り立つ. $i > 0$ とし, $L_i(G) \leq Z_{n-i+1}(G)$ とすると, $Z_i(G)$ の定義より,

$$L_{i+1}(G) = [L_i(G), G] \leq [Z_{n-i+1}(G), G] \leq Z_{n-i}(G).$$

従って, 上の主張を得る. 特に, $L_{n+1}(G) \leq Z_0(G) = \{1\}$ であり, G は冪零群となり, $m \leq n \leq k$. 特に, $k = m$. □

系 1.7.25 $G \neq \{1\}$ が m 級の冪零群である為の必要十分条件は $G/Z(G)$ が $m-1$ 級の冪零群となることである.

問 1.7.26 二つの冪零群の直積は冪零群であることを示せ.

命題 1.7.27 p-群は冪零群である.

証明 G を最小位数の反例とする. $G \neq 1$ であり, $Z(G) \neq 1$. G の最小性より, $G/Z(G)$ は冪零群である. すると, 系 1.7.25 より, G も冪零群となり, 不合理である. □

命題 1.7.28 G を m 級の冪零群とする. G の部分群, G の準同型像は高々 m 級の冪零群である.

証明 $H \leq G$ とすると, $L_{m+1}(H) \leq L_{m+1}(G) = 1$. 従って, H は高々 m 級の冪零群である. $f : G \longrightarrow K$ が群全射ならば, $1 = f(L_{m+1}(G)) = L_{m+1}(K)$. 従って, K は高々 m 級の冪零群である. □

命題 1.7.29 G は冪零群とする. このとき,

$$H < G \quad \Longrightarrow \quad H < N_G(H).$$

特に, 冪零群の極大部分群は正規である.

証明 $G = Z_m(G) \geq Z_{m-1} \geq \cdots \geq Z_1(G) \geq Z_0(G) = 1$ を考える. このとき, $H \not\supset Z_i(G), H \supset Z_{i-1}(G)$ $(\exists i < m)$. このとき, $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ なので, $Z_i(G)/Z_{i-1}(G) \leq N(H/Z_{i-1}(G))$. 従って, $Z_i(G) \leq N_G(H)$ となり, $H < N_G(H)$ でなければならない. □

定理 1.7.30 有限群 G について次は同値である：

(1) G は冪零群である.

(2) $\Phi(G) \geq G^{(1)} = [G, G]$.

(3) G の Sylow 部分群は正規である.

(4) G は Sylow 部分群の直積である.

証明 (1) $\Longrightarrow$ (2) 命題 1.7.29 より, G の極大部分群 M は正規である. G/M は非自明な部分群をもたないので, 素数位数のアーベル群である. よって, 補題 1.7.11 より, $M \geq [G, G]$. M は任意なので, $\Phi(G) \geq [G, G]$. (2) $\Longrightarrow$ (3) P を Sylow 部分群とする. $P \not\trianglelefteq G$ とすると, $P < N_G(P) < G$. $N_G(P)$ を含む極大部分群を M とすると, $M \geq [G, G]$. $M \triangleleft G$ なので Frattini 論法 (補題 1.6.18) より, $G = M \cdot N_G(P) = M$. これは不合理であり, $G = N_G(P)$ を得る. (3) $\Longrightarrow$ (4) $|G| = p_1^{e_1} \cdots p_n^{e_n}$ を素因数分解とする. 仮定より, p_i-Sylow 群 P_i は唯一つであり, $[P_i, P_j] \leq P_i \cap P_j = 1$ $(i \neq j)$. $P_1 \cdots P_i \trianglelefteq G$ であり, 補題 1.5.20 より, $|P_1 \cdots P_i| = p_1^{e_1} \cdots p_i^{e_i}$, $P_1 \cdots P_i \cap P_{i+1} = 1$ $(\forall i)$. 従って,

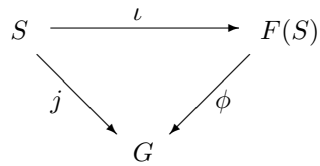
$$P_1 \times \cdots \times P_n \longrightarrow G; \quad (a_1, \cdots, a_n) \longmapsto a_1 \cdots a_n$$

は群同型射である. (4) $\Longrightarrow$ (1) p-群は冪零群であり, 冪零群の直積は冪零群である. □

1.8 自由群

1.8.1 定義と構成

S を集合とし, $\iota : S \longrightarrow F(S)$ を S から群 $F(S)$ への集合としての写像とする. S から群への写像 $j : S \longrightarrow G$ が任意に与えられたとき, 次が可換図となる群射 $\phi : F(S) \longrightarrow G$ が一意的に存在するとき, 写像 $\iota : S \longrightarrow F(S)$, または $F(S)$ を S **上の自由群** という：



命題 1.8.1 S を集合とし, $(\iota, F(S))$ を S 上の自由群とする. このとき, 次が成り立つ：

(1) ι は単射である.

(2) $\langle \iota(S) \rangle = F(S)$.

(3) $\iota' : S \longrightarrow F'$ も S 上の自由群とすると, 群同型射 $\phi : F(S) \longrightarrow F'$ で, $\phi \circ \iota = \iota$, を満たすものが一意的に存在する.

証明 (1) $s, t \in S$ を異なる二元とし, $G = \{1, -1\}$ を位数 2 の群とする. $j : S \longrightarrow G$ を $j(s) = 1, j(S - \{s\}) = -1$ と定める. このとき, 定義より, 群射 $\phi : F(S) \longrightarrow G$ で, $\phi \circ \iota = j$ を満たすものが存在する. すると,

$$1 = j(s) = \phi(\iota(s)) \neq -1 = j(t) = \phi(\iota(t)).$$

従って, $\iota(s) \neq \iota(t)$ を得る. よって, ι は単射である.

(2) $H = \langle \iota(S) \rangle$ とする. 写像 $\iota : S \longrightarrow F(S)$ の終集合を H とした写像を ι' とし, $j : H \longrightarrow F(S)$ を自然な群単射とする. このとき, 定義より, 群射 $\phi : F(S) \longrightarrow H$ で, $\phi \circ \iota = \iota'$ を満たすものが一意的に存在する. やはり, 定義より, 恒等写像 $I = I_{F(S)} : F(S) \longrightarrow F(S)$ は, $I \circ \iota = \iota$ を満たす唯一つの群射である. 群射 $j \circ \phi : F(S) \longrightarrow F(S)$ は,

$$j \circ \phi \circ \iota = j \circ \iota' = \iota$$

を満たすので, $j \circ \phi = I$. I は全射なので, j は全射であり, $H = F(S)$.

(3) 定義より, 群射 $\phi : F(S) \longrightarrow F'$ で, $\phi \circ \iota = \iota'$ を満たすものが一意的に存在する. (ι', F') も S 上の自由群なので, 群射 $\psi : F' \longrightarrow F(S)$ で, $\psi \circ \iota' = \iota$ を満たすものが一意的に存在する. 従って,

$$\psi \circ \phi \circ \iota = \psi \circ \iota' = \iota.$$

$\iota \circ I = \iota$ を満たす群射 $I = I_{F(S)} : F(S) \longrightarrow F(S)$ の一意性により, $I = \psi \circ \phi$. 同様にして, $I_{F'} = \phi \circ \psi$ を得る. 特に, ϕ は群同型射である. □

$S = \{a, b, c \cdots\}$ を記号 $a, b, \cdots$ の集合とし, S に含まれる有限個の元（重複も許す）からなる列を **語** という. 例えば,

$$a,\ ab,\ ba,\ cbabba, \cdots$$

0 個の語も許すことにし, それを 1 と表す. 語の全体のなす集合を $W(S)$ で表すことにする. 二つの語 w_1, w_2 の積を $w_1 w_2$ により定義する. 例えば, $w_1 = ba, w_2 = cab$ のとき, $w_1 w_2 = bacab$ である. すると, $(W(S); \cdot)$ は, 1 を単位元とする単位半群をなす.

群を構成するのであるから, 逆元を作らねばならない. そこで, S の各元 a に対し, 全く新しい記号 a^{-1} を導入し, $S^{-1} = \{a^{-1}, b^{-1}, \cdots\}$ とし, $S_0 = S \cup S^{-1}$ とする. 新しい記号を導入したので, $S \cap S^{-1} = \emptyset$ が満たされている.

S から語を作ったように, 今度は, S_0 から語を作りその全体を W' と表す. W' の二つの元に関係を導入する：

$$w = x_1 \cdots x_n \in W' \quad (x_i \in S_0)$$

に対し,

$$x_{i+1} = x_i^{-1} \quad \text{又は} \quad x_i = x_{i+1}^{-1}$$

となる i が存在したとき,

$$w' := x_1 \cdots x_{i-1} x_{i+2} \cdots x_n$$

を w から簡約されて得られた語という. また, 上の様な i が存在しないとき, w は **被約** であるという. 1 も被約とする.

補題 1.8.2 与えられた語 $w \in W'$ に何度か簡約をし被約な語 w_0 を得る. 更に, w_0 は簡約の仕方によらない.

証明 $w = x_1 \cdots x_n$ $(x_i \in S_0)$ と表したとき, n に関する帰納法で, 補題を示す. $n = 0, 1$ のときは明らかである. $n \geq 2$ とし, $n-1$ 以下の場合は, 補題は正しいとする.

一番目の仕方で行う簡約の操作を $\rho_1, \rho_2, \cdots, \rho_k$ とし, この操作により得られる語を $\rho_1(w) = w_1, \rho_2(\rho_1(w)) = w_2, \cdots$ と表す. 二番目の仕方で行う簡約の操作を $\tau_1, \tau_2, \cdots, \tau_l$ とし, $\tau_1(w) = w'_1, \tau_2(\tau_1(w)) = w'_2, \cdots$ と表す. 従って, 示すべきことは, $w_k = w'_l$ である. ρ_1 で, $x_i x_{i+1}$ が簡約されたとし, τ_1 で, $x_j x_{j+1}$ が簡約されたとする. $i = j$ ならば, $\rho_1(w) = \tau_1(w)$ なので, 帰納法の仮定により, $w_k = w'_l$ を得る. そこで, $i < j$ と仮定して良い. $i + 1 < j$ ならば, $\tau_1(w_1) = \rho_1(w'_1)$. 帰納法の仮定により, w_1, w'_1 を簡約して得られる被約な語 w'' は簡約の仕方によらない. よって, $w_k = w'' = w'_l$ を得る. よって, $i + 1 = j$ として良い. このとき, (x_i, x_{i+1}, x_{i+2}) は, ある $s \in S$ が存在し,

$$(s, s^{-1}, s) \quad \text{又は} \quad (s^{-1}, s, s^{-1})$$

に等しい. 前者の場合,

$$w_1 = \rho_1(w) = x_1 \cdots x_{i-1} s x_{i+2} \cdots x_n = \tau_1(w) = w'_1.$$

従って, 帰納法の仮定により, $w_k = w'_l$. 後者の場合も同様である. よって補題が示された. □

語 $w \in W'$ に対し, 補題により確定した被約な語 w_0 を, w の **被約形** という. 二つの語 w, w' に対し, その被約形が一致するとき, w と w' は同値であるといい, $w \sim w'$ と表す. この関係は同値関係であり, 各 $w \in W'$ に対し, w を含む同値類を $[w]$ で表す. また, 互いに異なる同値類全体の集合, 即ち, W' を関係 $\sim$ で割った商集合 $W'/\sim$ を $F(S)$ と表す.

補題 1.8.3 $F(S)$ の二つの元 $[w], [w']$ に対し, $[ww']$ は代表元 w, w' の取り方によらない.

証明 $[w] = [w_1], [w'] = [w'_1]$ と仮定する. このとき, w, w_1 は共通の被約形 w_0 を持ち, w', w'_1 も共通の被約形 w'_0 を持つ. 従って, $[w] = [w_1] = [w_0], [w'] = [w'_1] = [w'_0]$. $w_0 w'_0$ の被約形を $(w_0 w'_0)_0$ とすれば,

$$[ww'] = [w_0 w'_0] = [(w_0 w'_0)_0] = [w_1 w'_1]$$

を得て, 補題が示された. □

定理 1.8.4 $F(S)$ の二元 $[w], [w']$ の積を $[ww']$ とすることにより, $F(S)$ は群をなす. 更に, $\iota(s) = [s]$ と定めると, $(\iota, F(S))$ は S 上の自由群である.

証明 $[w], [w'], [w''] \in F(S)$ に対し,

$$([w][w'])[w''] = [((ww')w'')_0] = [(w(w'w''))_0] = [w]([w'][w'']).$$

但し, $((ww')w'')_0$ は, 語 $(ww')w''$ の被約形である. $[1]$ が単位元であり, $[x_1 \cdots x_n]^{-1} = [x_n^{-1} \cdots x_1^{-1}]$ である.

さて, $j : S \longrightarrow G$ を群 G への写像とする. $F(S)$ の任意の元

$$a = [s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}] \quad (\epsilon_i \in \{1, -1\})$$

に対し,

$$\phi(a) = j(s_1)^{\epsilon_1} \cdots j(s_n)^{\epsilon_n}$$

と定める. すると, $\phi(a)$ は代表元の取り方によらず, ϕ は群射である. また, ϕ の一意性は明らかである. □

1.8.2 生成系と基本関係式

G を群として S を G の生成系とする：$G = \langle S \rangle$. $(\iota, F(S) : S \longrightarrow F(S)$ を集合 S 上の自由群とする. このとき, $j : S \longrightarrow G$ を自然な単射とするとき, 群射 $\phi : F(S) \longrightarrow G$ で, $j = \phi \circ \iota$ を満たすものが一意的に存在する. すると, $G = \langle S \rangle$ なので, ϕ は群全射である. 特に, G 自身は, G の生成系なので, 次を得る：

命題 1.8.5 任意の群 G に対し, 自由群 F と群全射 $F \longrightarrow G$ が存在する.

群全射 $\phi : F(S) \longrightarrow G = \langle S \rangle$ に, 同型定理を適用し,

$$F(S)/N \simeq G \quad (N = \mathrm{Ker}(\phi)).$$

N の任意の元は, 被約な語

$$s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \quad (\epsilon_i \in \{1, -1\})$$

を含む同値類として表される. N の, 正規部分群としての, 生成系を

$$\{[w_\lambda] \mid \lambda \in \Lambda, w_\lambda \text{ は被約 } \}$$

と表す. このとき,

$$R = \{w_\lambda = 1 \mid \lambda \in \Lambda\}$$

を **基本関係式** の集合といい, 群 G を

$$G = \langle S \mid R \rangle$$

と表す.

定理 1.8.6 $G = \langle S \mid R \rangle$ とする. $j : S \longrightarrow S'$ を集合の全射とし, $G' = \langle S' \rangle$ とする. R の任意の元

$$s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} = 1 \quad (\epsilon_i \in \{1, -1\})$$

に対し,

$$j(s_1)^{\epsilon_1} \cdots j(s_n)^{\epsilon_n} = 1$$

を満たすならば, 群全射 $\phi : G \longrightarrow G'$ が存在する.

証明　$\iota : S \longrightarrow F(S)$ を S 上の自由群とする．従って, $j : S \longrightarrow S' \subset G'$ に対し, 群全射 $\psi : F(S) \longrightarrow G'$ が存在し, $\phi \circ \iota = j$ を満たす．このとき, $\psi(r) = 1$ $(\forall r = 1 \in R)$ を満たす．従って, $\psi(N) = \{1\}$ となり, 剰余群の性質から, ψ は剰余群 $G = F(S)/N$ を経由する．即ち, 群全射 $\phi : F(S)/N = G \longrightarrow G'$ が存在し, $\phi \circ \pi = \psi$ を満たす．但し, $\pi : F(S) \longrightarrow F(S)/N = G$ は自然な群全射である．　□

今までの議論から, 次が得られる：

命題 1.8.7　S を集合とし, $\tilde{R}$ を被約な語の集合とし, $R = \{w = 1 \mid w \in \tilde{R}\}$ とする．$\tilde{R}$ を含む $F(S)$ の最小の正規部分群を N とするとき,

$$F(S)/N = \langle S \mid R \rangle$$

となる．

例題 1.8.8　n を自然数とするとき,

$$G = \langle x, y \mid x^n = y^2 = yxyx = 1 \rangle$$

は, 位数 $2n$ の二面体群 D_{2n} に同型である．

（解）　uv 平面の角 $2\pi/n$ の回転を ρ_n と表し, u 軸に関する角 π の回転を r と表す．このとき, $D_{2n} = \langle \rho_n, r \rangle$ である．$S = \{x, y\}$ とし, $\iota : S \longrightarrow F(S)$ を S 上の自由群とする．

$$j(x) = \rho_n, \quad j(y) = r$$

とすると, 群全射 $\psi : FS \longrightarrow D_{2n}$ が存在し, $\psi(x) = \rho_n, \psi(y) = r$ を満たす．

$$\psi(x^n) = 1, \quad \psi(y^2) = 1, \psi(yxyx) = 1$$

なので, 定理 1.8.6 より, 群全射 $\phi : F(S)/N \longrightarrow D_{2n}$ が存在する．但し, N は, $\tilde{R} = \{x^n, y^2, yxyx\}$ を含む最小の正規部分群である．$F(S)/N$ の元は

$$1, x, \cdots, x^{n-1}, y, yx, \cdots, yx^{n-1}$$

のいずれかである．実際, $F(S)/N$ においては, $xy = yx^{n-1}$ が成り立つので, y の前にある x は, y の後ろへ移動できる．従って, $|F(S)/N| \leq 2n$ であり, $|D_{2n}| = 2n$ なので, $|F(S)/N| = 2n$．よって, ϕ は同型射である．　□

例題 1.8.9　（n 次対称群）$S = \{x_1, \cdots, x_{n-1}\}$ とし, R を次の集合とする：

$$\begin{array}{ll} x_1^2 = \cdots = x_{n-1}^2 = 1 & \\ (x_{i+1}x_i)^3 = 1 & (1 \leq i \leq n-2) \\ (x_i x_j)^2 = 1 & (|i-j| > 1) \end{array}$$

このとき,

$$\langle S \mid R \rangle \simeq S_n.$$

（解） $y_i = (i\ i+1)$ とすると, 命題 1.3.14 より,

$$S_n = \langle y_1, \cdots, y_{n-1} \rangle.$$

また, 容易に判るように, $y_1, \cdots, y_{n-1}$ は, 上の関係式を満たす. 従って, 群全射 $\phi : G_n := \langle S \mid R \rangle \longrightarrow S_n$ が存在する.

次に, $G_n \simeq S_n$ を, n に関する帰納法で示す. $n = 2$ のとき, $G_2 = \langle x_1 \mid x_1^2 = 1 \rangle$ は位数 2 の群である. $n > 2$ として, $n-1$ のときは正しいとする. $H = \langle x_2, \cdots, x_{n-1} \rangle \leq G$ とすると, 帰納法の仮定により, $S_{n-1} = H$.

$$H_1 = H,\ H_2 = H_1 x_1, H_3 = H_2 x_2,\ \cdots,\ H_n = H_{n-1} x_{n-1}$$

とする. このとき,

(1) $H_i x_i = H_{i+1} \quad (1 \leq i \leq n-1)$,

(2) $H_i x_{i-1} = H_{i-1} \quad (2 \leq i \leq n)$,

(3) $H_i x_j = H_i \quad (j \neq i, i-1)$

を示す. (1), (2) は, H_i の定義から直ちに得られる. $j > i$ とすると, 仮定より, $1 \leq k \leq i-1$ ならば $(x_k x_j)^2 = 1$ 即ち, $x_k x_j = x_j x_k$. 従って, $j \geq 2$ であり, $H x_j = H$ が成り立つので,

$$H_i x_j = H x_1 \cdots x_{i-1} x_j = H x_j x_1 \cdots x_{i-1} = H_i.$$

また, 仮定 $(x_{i+1} x_i)^3 = 1$ より,

$$x_j x_{j+1} x_j = x_{j+1} x_j x_{j+1}.$$

従って, $j < i-1$ とすると,

$$\begin{aligned} H_i x_j &= H x_1 \cdots x_{i-1} x_j \\ &= H x_1 \cdots x_j x_{j+1} x_j x_{j+2} \cdots x_{i-1} \\ &= H x_1 \cdots x_{j-1} x_{j+1} x_j x_{j+1} x_{j+2} \cdots x_{i-1} \\ &= H x_j x_1 \cdots x_{j-1} x_j x_{j+1} x_{j+2} \cdots x_{i-1} = H_i. \end{aligned}$$

よって, 任意の i, j に対し, ある k が存在して

$$H_i x_j = H_k.$$

従って, H の任意の右剰余類は $H_1, \cdots, H_n$ のいずれかに一致する. よって, $|G_n| \leq |H| \cdot |G/H| \leq n!$ となり, $G_n \simeq S_n$. □

例題 1.8.10 （n 次交代群）$n \geq 3$ とする. $S = \{y_1, \cdots, y_{n-2}\}$ とし, R を次の集合とする：

$$\begin{array}{ll} y_1^3 = y_2^2 = \cdots = y_{n-2}^2 = 1 & \\ (y_i y_{i+1})^3 = 1 & (1 \leq i \leq n-3) \\ (y_i y_j)^2 = 1 & (|i-j| > 1) \end{array}$$

このとき,

$$\langle S \mid R \rangle \simeq A_n.$$

（解） $s_1 = (1\ 2\ 3), s_{i-1} = (1\ 2)(i\ i+1)\ (3 \leq i \leq n-1)$ とすると, 例題 **??** より,

$$A_n = \langle s_1, \cdots, s_{n-1} \rangle.$$

また, 容易に判るように, $s_1, \cdots, s_{n-2}$ は, 上の関係式を満たす. 従って, 群全射 $\phi : G_n := \langle S \mid R \rangle \longrightarrow A_n$ が存在する.

次に, $G_n \simeq A_n$ を, n に関する帰納法で示す. $n = 3$ のとき, $G_3 = \langle y_1 \mid y_1^3 = 1 \rangle$ は位数 3 の群である. $n > 3$ として, $n-1$ のときは正しいとする. $H = \langle y_1, \cdots, y_{n-3} \rangle \leq G_n$ とする. このとき, 帰納法の仮定により, $A_{n-1} = H$.

$$H_n = H,\ H_{n-1} = H_n y_{n-2}, H_{n-2} = H_{n-1} y_{n-3},\ \cdots,\ H_2 = H_3 y_1,\ H_1 = H_2 y_1$$

とする. このとき, 前の例題と同様にして, 次が成り立つ：

(1) $H_i y_{i-2} = H_{i-1} \quad (3 \leq i \leq n)$,

(2) $H_i y_{i-1} = H_{i+1} \quad (3 \leq i \leq n)$,

(3) $H_2 y_1 = H_1$,

(4) $H_i y_j = H_i \quad (j \neq i-1, i-2)$.

よって, 任意の i, j に対し, ある k が存在して

$$H_i y_j = H_k.$$

従って, H の任意の右剰余類は $H_1, \cdots, H_n$ のいずれかに一致する. よって, $|G_n| \leq |H| \cdot |G/H| \leq n!/2$ となり, $G_n \simeq A_n$. □

1.9 アーベル群

この節では, アーベル群の演算は加法で表す.

1.9.1 自由アーベル群

定義 1.9.1 A をアーベル群とする. A に含まれる $u_1, \cdots, u_n$ は, 次を満たすとき, **一次独立** であるという：

$$m_1 u_1 + \cdots + m_n u_n = 0\ (m_1, \cdots, m_n \in \mathbb{Z}) \quad \Longrightarrow \quad m_1 = \cdots = m_n = 0.$$

定義 1.9.2 A をアーベル群とする. A に含まれる元の列 $(u_1, \cdots, u_n)$ は, 次を満たすとき, A の **基底** と呼ばれる.

(1) $A = \langle u_1, \cdots, u_n \rangle$,

(2) $\{u_1, \cdots, u_n\}$ は一次独立である.

例 1.9.1 $\mathbb{Z}$ の n 個の直和 $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ において

$$\mathbf{e}_1 = (1, 0, 0, \cdots, 0),\ \mathbf{e}_2 = (0, 1, 0, \cdots, 0),\ \cdots,\ \mathbf{e}_n = (0, 0, \cdots, 0, 1)$$

は基底である. これを **標準基底** という.

補題 1.9.3 A をアーベル群とするとき, 次は同値である.

(1) A は n 個の元からなる基底を持つ.

(2) A は $\mathbb{Z}^n$ に同型である.

このとき, 基底をなす元の個数は, 基底の取り方によらない.

証明 $u_1, \cdots, u_n$ を A の基底とするとき

$$f : \mathbb{Z}^n \longrightarrow A, \quad (m_1, \cdots .m_n) \longmapsto m_1u_1 + \cdots + m_nu_n$$

は同型写像を与える. 逆は, 上の例から直ちに得られる.

次に最後の部分を示す. 素数 p を一つ固定し, 準同型写像

$$p_A : A \longrightarrow A, \quad x \longmapsto px, \quad p : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n, \quad x \longmapsto px$$

を考える. すると, 次の図は可換である:

$$\begin{array}{ccccc} & & p_A & & \\ & A & \longrightarrow & A & \\ f & \downarrow & & \downarrow & f\ . \\ & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n & \\ & & p & & \end{array}$$

このとき, $A/\mathrm{Im}(p_A) \simeq \mathbb{Z}^n/\mathrm{Im}(p) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ であり, これらの群の位数は p^n となり, 基底のとり方によらない. □

問 1.9.4 $A/\mathrm{Im}(p_A) \simeq \mathbb{Z}^n/\mathrm{Im}(p)$ を証明せよ.

定義 1.9.5 上の定理の条件を満たすアーベル群を **階数** n **の自由アーベル群** という. 自明な群 $\{0\}$ は階数 0 の自由アーベル群とする.

例 1.9.2 $\mathbb{Z}$ の部分群は $\{0\}$ であるか, または $(d) = d\mathbb{Z}$ $(d \in \mathbb{N})$ と表される. $(d) \simeq \mathbb{Z}$ なので, $\mathbb{Z}$ の部分群は, 自由アーベル群であり, その階数は 1 または 0 である.

補題 1.9.6 F を階数 n の自由アーベル群とし, A をその部分群とする. このとき A は, 階数が n 以下の自由アーベル群である.

証明 F の階数 n に関する帰納法で示す. $n = 1$ の場合は, 上の例である. $n > 1$ とする. $(u_1, \cdots, u_n)$ を F の基底とし, 全射準同型写像

$$f : F \longrightarrow \mathbb{Z}, \quad c_1u_1 + \cdots + c_nu_n \longmapsto c_1$$

の核 $B = \mathrm{Ker}(f) = \langle u_2, \cdots, u_n \rangle$ は階数 $n-1$ の自由アーベル群である. f の A への制限写像を g と表す:

$$g = f|_A : A \longrightarrow f(A).$$

すると, $\mathrm{Ker}(g) = B \cap A \leq B$. 帰納法の仮定により, $B \cap A$ は階数 $n-1$ 以下の自由アーベル群である. また, $f(A)(\leq \mathbb{Z})$ は階数が 1 以下の自由アーベル群である.

$f(A) = 0$ のとき, $B = A$ であり, A は階数 $n-1$ の自由アーベル群である. $f(A) = (d)$ $(d \neq 0)$ とする. g は全射なので, $g(a_0) = d$ となる $a_0 \in A$ が存在する. 一方 $B \cap A$ の基底を $(a_1, \cdots, a_m)$ $(m \leq n-1)$ とする. このとき, $\{a_0, a_1, \cdots, a_m\}$ は, 一次独立であることを示そう.

$$x := \sum_{i=0}^{m} c_ia_i = 0 \quad (c_i \in \mathbb{Z})$$

とする. このとき, $0 = f(x) = c_0d$. $d \neq 0$ なので, $c_0 = 0$. また, $(a_1, \cdots, a_m)$ は基底なので, $c_1 = \cdots = c_m = 0$. よって, $\{a_0, a_1, \cdots, a_m\}$ は一次独立である.

次に, $A = \langle a_0, a_1, \cdots, a_m \rangle$ A を示そう. $x \in A$ を任意に取る. $f(x) = c_0d$ とし, $y = x - c_0a_0$ とすると, $f(y) = f(x) - c_0d = 0$. 従って, $y \in B \cap A$ となり,

$$y = \sum_{i=1}^{m} c_ia_i$$

と表される. 従って, $x = c_0a_0 + c_1a_1 + \cdots + c_ma_m$. よって, $(a_0, a_1, \cdots, a_m)$ は, A の基底であり, A は階数が $1 + n - 1 = n$ 以下の自由アーベル群である. □

1.9.2 有限生成アーベル群の基本定理

この節では, 次の定理を用いて, 有限生成アーベル群の基本定理を証明する.

定理 1.9.7 任意の整数行列 $M \in \mathrm{M}_{m \times n}(\mathbb{Z})$ は次の形の行列に対等である：

$$\begin{pmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_l & \\ & & & & O \end{pmatrix}, \quad 0 < e_i | e_{i+1} \quad (i = 1, 2, \cdots l-1).$$

集合 $\{e_1, \cdots, e_l\}$ は M により一意的に定まる. $\{e_1, \cdots, e_l\}$ を M の **単因子** という.

注意 1.9.1 この定理の証明については, 線形代数学 2 講義ノートを参照せよ.

アーベル群 A が有限生成であるとは,

$$A = \langle a_1, \cdots, a_n \rangle \quad (\exists a_1, \cdots, a_n \rangle).$$

問 1.9.8 次は同値であることを示せ.

(1) A を有限生成アーベル群.

(2) 負でない整数 n と全射準同型写像 $f : \mathbb{Z}^n \longrightarrow A$ が存在する.

定理 1.9.9 （有限生成アーベル群の基本定理）有限生成アーベル群は, 次の形の群に同型である.

$$\mathbb{Z}/(e_1) \oplus \cdots \oplus \mathbb{Z}/(e_r) \oplus \mathbb{Z}^r, \quad e_i | e_{i+1} (1 \leq i < r)$$

右辺に現れる $\mathbb{Z}$ の個数 r と $e_1, \cdots e_l$ は ± 1 倍を除いて一意的に定まる.

証明 A を有限生成アーベル群とすると, 全射

$$f : \mathbb{Z}^n \longrightarrow A$$

が存在する. 定理 1.9.6 により, $B := \mathrm{Ker}(f)$ は, 階数 n 以下の自由アーベル群である. また, 同型定理より,

$$\mathbb{Z}^n/B \simeq A.$$

さて, $(b_1, \cdots, b_l)$ を B の基底とする:

$$b_1 = (x_{11}, \cdots, x_{1n}), \cdots, b_m = (x_{m1}, \cdots, x_{mn})$$

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = X \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}, \quad X = (x_{ij}) \in \mathrm{M}_{m \times n}(\mathbb{Z}).$$

$(b_1, \cdots, b_m)$ は, B の基底なので, $\mathrm{X} = m$ に注意する. 行列 X に, 定理 1.9.7 を適用し,

$$PXQ = \begin{pmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_m & \\ & & & & O \end{pmatrix}, \quad e_i | e_{i+1} \quad (i = 1, 2, \cdots m-1)$$

となる

$$P \in \mathrm{GL}_m(\mathbb{Z}), \quad Q \in \mathrm{GL}_n(\mathbb{Z})$$

が存在する.

$$\begin{pmatrix} b'_1 \\ \vdots \\ b'_m \end{pmatrix} = P \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \quad \begin{pmatrix} \mathbf{e}'_1 \\ \vdots \\ \mathbf{e}'_n \end{pmatrix} = Q^{-1} \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}$$

と基底を変換すると,

$$B \simeq (e_1) \oplus \cdots \oplus (e_l) \leq \mathbb{Z}^l \oplus \mathbb{Z}^r \simeq \mathbb{Z}^n.$$

従って,

$$A \simeq \mathbb{Z}^n/B \simeq \mathbb{Z}/(e_1) \oplus \cdots \mathbb{Z}/(e_l) \oplus \mathbb{Z}^r.$$

□

定義 1.9.10 A をアーベル群とする. A に含まれる位数有限の元全体のなす部分群を A_{tor} と表し, A の **捩れ部分群** という. $A_{tor} = 0$ を満たす群を, **捩れがない** という. また, $A = A_{tor}$ となるとき, A を **捩れ群** という.

問 1.9.11 A_{tor} は部分群をなすことを示せ.

例 1.9.3 A は捩れのないアーベル群とし, $u\ (\neq 0) \in A$ とする. このとき, $\{u\}$ は一次独立である.

問 1.9.12 A は捩れのないアーベル群とする. 任意の自然数 c に対し, 準同型写像

$$c_A : A \longrightarrow A, \quad x \longmapsto cx$$

は単射であることを確認せよ.

例 1.9.4

$$A \simeq \mathbb{Z}/(e_1) \oplus \cdots \oplus \mathbb{Z}/(e_l) \oplus \mathbb{Z}^r \quad (e_1|e_2|\cdots|e_l)$$

を有限生成アーベル群とする. このとき,

$$A_{tor} \simeq \mathbb{Z}/(e_1) \oplus \cdots \oplus \mathbb{Z}/(e_l)$$

は有限アーベル群であり,

$$A/A_{tor} \simeq \mathbb{Z}^r$$

は階数 r の自由アーベル群である. 特に r は, A により, 一意的に定まる. r を有限生成アーベル群 A の **階数** という

問 1.9.13 捩れがない有限生成アーベル群は自由アーベル群であることを確かめよ.

例 1.9.5 F を階数 n の自由アーベル群とし, $A \leq F$ を階数 n 部分群とする. $(f_1, \cdots, f_n)$, $(a_1, \cdots, a_n)$ を F, A の基底とする.

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}, \quad M \in \mathrm{M}_n(\mathbb{Z})$$

とするとき,

$$|F : A| = |\det(M)|.$$

1.9.3 有限アーベル群

素数冪位数の巡回群は

$$\mathbb{Z}/(p^e), \quad p: \text{素数}$$

に同型である. 任意のアーベル群はこれらの群の直和に同型であることを示す.

有限アーベル群に, 有限生成アーベル群の基本定理を適用すると, 次を得る.

補題 1.9.14 A を有限アーベル群とすると, $e_i|e_{i+1}$ $(i = 1, \cdots l-1)$ を満たす自然数 $e_1, \cdots, e_l$ が存在し,

$$A \simeq \mathbb{Z}/(e_1) \oplus \cdots \oplus \mathbb{Z}/(e_l).$$

ここで, 中国剰余定理を思い出す:

定理 1.9.15 （中国剰余定理）$m_1, \cdots, m_r$ を

$$(m_i, m_j) = 1 \ \ (i \neq j)$$

を満たす自然数とし, $m = m_1 \cdots m_r$ とする. このとき,

$$\mathbb{Z}/(m) \simeq \mathbb{Z}/(m_1) \oplus \cdots \oplus \mathbb{Z}/(m_r).$$

特に, $m = p_1^{i_1} \cdots p_r^{i_r}$ $(p_i \neq p_j \ (i \neq j))$ を m の素因数分解とするとき,

$$\mathbb{Z}/(m) \simeq \mathbb{Z}/(p_1^{i_1}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{i_r}).$$

注意 1.9.2 この定理の証明については, 線形代数学２講義ノートを参照せよ.

定義 1.9.16 A を有限アーベル群とする. 素数 p に対し, 部分群 A_p を次のように定める.

$$A_p = \{x \in A \mid \mathrm{ord}(x) = p \text{ 冪 }\}$$

と定める.

定理 1.9.17 A を有限アーベル群とし, $|A| = p_1^{i_1} \cdots p_r^{i_r}$ を素因数分解とする. このとき

$$A \simeq A_{p_1} \oplus \cdots \oplus A_{p_r}$$

であり, 適当な負でない整数 k_i $(1 \leq k \leq l, 1 \leq i \leq r)$ が存在して,

$$A_{p_i} \simeq \mathbb{Z}/(p_i^{1_i}) \oplus \cdots \oplus \mathbb{Z}/(p_i^{l_i}) \quad (0 \leq 1_i \leq \cdots \leq l_i).$$

証明 補題 1.9.14 より,

$$A \simeq \mathbb{Z}/(e_1) \oplus \cdots \oplus \mathbb{Z}/(e_l).$$

$$e_k = p_1^{k_1} \cdots p_r^{k_r}$$

（$k_i = 0$ の場合も有りうる）を素因数分解とすれば,

$$A \simeq (\mathbb{Z}/(p_1^{1_1}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{1_r})) \oplus \cdots \oplus (\mathbb{Z}/(p_1^{l_1}) \oplus \cdots \mathbb{Z}/(p_r^{l_r})).$$

このとき,

$$A_{p_i} \simeq \mathbb{Z}/(p_i^{1_i}) \oplus \cdots \mathbb{Z}/(p_i^{l_i}).$$

□

定義 1.9.18 p を素数とする. 位数が p 冪のアーベル群を **アーベル p-群** という.

次に, 有限アーベル p-群の構造を調べよう. 以下しばらくの間, 素数 p を固定して話を進める.

例 1.9.6 $A = \mathbb{Z}/(p^r)$ とする. 準同型写像

$$p_A : A \longrightarrow A, \quad x \longmapsto px$$

を考える. このとき,

$$\mathrm{Im}(p_A) = pA = \{px \mid x \in A\} \simeq \mathbb{Z}/(p^{r-1}).$$

定理 1.9.19 A を有限アーベル p 群とする. このとき

$$A \simeq \mathbb{Z}/(p^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r}), \quad 1 \leq e_1 \leq e_2 \leq \cdots e_r.$$

さらに, $(e_1, \cdots, e_r)$ は一意的に定まる.
このとき, A を $(p^{e_1}, \cdots, p^{e_r})$ **型** のアーベル群という.

証明 前半は, 定理 1.9.17 から直ちに得られる.
次に, 位数に関する帰納法で, 一意性を示す.

$$\begin{aligned} A &\simeq \mathbb{Z}/(p^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r}), \quad 1 = e_1 = \cdots = e_k < e_{k+1} \leq \cdots \leq e_r \\ &\simeq \mathbb{Z}/(p^{f_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{f_s}), \quad 1 = f_1 = \cdots = f_l < f_{l+1} \leq \cdots f_s \end{aligned}$$

とする. このとき

$$\begin{aligned} pA &\simeq \mathbb{Z}/(p^{e_{k+1}-1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r-1}) \\ &\simeq \mathbb{Z}/(p^{f_{1+1}-1}) \oplus \cdots \oplus \mathbb{Z}/(p^{f_s-1}). \end{aligned}$$

帰納法の仮定により,

$$r - k = s - l, \ e_{k+1} = f_{l+1}, \cdots e_r = e_s.$$

また A の位数を N とすると,

$$\log_p(N) = k + e_{k+1} + \cdots + e_r = l + e_{l+1} + \cdots + e_s.$$

従って $k = l$ となり, $r = s$. よって, 証明が終わる. □

第2章　環

整数全体の集合, 複素数を係数とし X を変数とする多項式全体の集合, 更に, 複素数を成分とする n 次正方行列の全体の集合には, 二つの二項演算「和」と「積」が定義され, 「足し算」, 「引き算」, 「掛け算」が, 二つの行列の積の順序は一般には変えられないけれども, 「自由に」出来る. このような対象を環という. この章では, 環にまつわる基本的概念を解説する.

2.1　環の定義

2.1.1　環の定義と例

定義 2.1.1 R を空でない集合とし,

$$+ : R \times R \longrightarrow R, \quad (x, y) \longmapsto x + y, \quad \times : R \times R \longrightarrow R, \quad (x, y) \longmapsto xy$$

を二項演算とする. これらの組 $(R; +, \times)$ は, 次の (R1), (R2), (R3) を満たすとき, **環** と呼ばれる：

(R1) $(R; +)$ は加法群をなす. 加法に関する単位元を 0 で表し **零元** という.

(R2) 積に関して, 次が成立つ：

(1) $(xy)z = x(yz), \quad (\forall x, y, z \in R)$,

(2) $x1 = 1x = x \quad (\forall x \in R)$ を満たす $1 \in R$ が存在する. 1 を乗法に関する **単位元** という.

(R3) （分配法則）

$$x(y + z) = xy + xz, \quad (x + y)z = xz + yz, \quad (\forall x, y, z \in R).$$

紛れる恐れがない場合は, 環 $(R; +, \cdot)$ を単に R と略記する.

注意 2.1.1 [1] 環 R に於いて, $1 = 0$ ならば $R = \{0\}$ となる. この環は例外的であり, **以下 $1 \neq 0$ と仮定する**. 従って環には少なくとも二元 $0, 1$ が含まれる.

環 R に対し, $R^+ := (R; +)$ を環 R の **加法群** という.

定義 2.1.2 積に関する交換法則

(R4)

$$xy = yx, \quad (\forall x, y \in R)$$

[1] $1 \neq 0$ を仮定しないこともあるので, 他書を参考にする場合は注意すること.

を満たす環を **可換環** という.

例 2.1.1 $+, \times$ を整数の和と積とするとき, $\mathbb{Z} = (\mathbb{Z}; +, \times)$ は, 可換環であり, **有理整数環** と呼ばれる.

例 2.1.2 有理数全体 $\mathbb{Q}$, 実数全体 R, 複素数全体 $\mathbb{C}$ も, 通常の和と積に関して, 可換環をなす.

例 2.1.3 複素数係数 n 次正方行列の全体 $\mathrm{M}_n(\mathbb{C})$ は, 行列の和と積に関して環をなす. $\mathrm{M}_n(\mathbb{C})$ を $\mathbb{C}$ 上の n 次 **行列環** という. 単位元は単位行列 I_n であり, 零元は零行列 O である.

例 2.1.4 V を複素数体 $\mathbb{C}$ 上の線形空間とする. V から V への線形写像の全体を $\mathrm{End}_{\mathbb{C}}(V) = \mathrm{End}(V)$ と表す. 和を

$$+ : \mathrm{End}(V) \times \mathrm{End}(V) \longrightarrow \mathrm{End}(V), \quad (f+g)(x) = f(x) + g(x) \ (\forall x \in V)$$

とし, 積を写像の合成

$$\circ : \mathrm{End}(V) \times \mathrm{End}(V) \longrightarrow \mathrm{End}(V), \quad (f \circ g)(x) = f(g(x)) \ (\forall x \in V)$$

とするとき, $(\mathrm{End}(V); +, \circ)$ は環をなす. これを, 線形空間 V の **自己準同型環** という.

例 2.1.3 を拡張して, 次を得る：

例 2.1.5 環 R の元を係数とする n 次正方行列の全体 $\mathrm{M}_n(R)$ は, 行列の和と積に関して環をなす. これを R 上の n 次 **行列環** という. 単位元は単位行列 I_n であり, 零元は零行列である. R が可換環であっても, $\mathrm{M}_n(R)$ は, $n \geq 2$ ならば, 非可換環である.

一般の環に於いては, $ab = 0$ だからといって $a = 0$ または $b = 0$ が成り立たないときが有る. 環 R の元 a は, $ab = 0$ $(\exists b \in R - \{0\})$ を満たすとき, **零因子** と呼ばれる. 0 以外に零因子を持たない可換環を **整域** という.

問 2.1.3 $M_n(\mathbb{C})$ の零因子を二つ挙げよ.

例 2.1.6 有理整数環 $\mathbb{Z}$ は整域である.

定義 2.1.4 環 R の部分集合 S が次を満たすとき, S を **部分環** という.

(SR1) 加法に関して S は部分群である.

(SR2) 乗法に関して S は閉じている.

(SR3) $1 \in S$.

例 2.1.7 $\mathbb{Z}$ は $\mathbb{Q}$ の部分環である. 同様に, $\mathbb{Q}$ は, $\mathbb{R}$ の, $\mathbb{R}$ は $\mathbb{C}$ の部分環である.

問 2.1.5 R を環とするとき, $\mathrm{Cent}(R) := \{x \in R \mid xy = yx \ (\forall y \in R)\}$ は, R の可換部分環をなすことを示せ. $\mathrm{Cent}(R)$ を R の **中心** という.

例 2.1.8 （関数環）集合 X から環 R への写像全体のなす集合を $\mathcal{F}(X,R)$ で表す．$f,g\in\mathcal{F}(X,R)$ に対し，それらの和 $f+g$ と積 fg を

$$(f+g)(x)=f(x)+g(x),\quad (fg)(x)=f(x)g(x),\quad \forall x\in X$$

により定めると，$\mathcal{F}(S,R)$ は環となり，X **上定義された** R**-値関数環** と呼ばれる．R が可換環ならば，$\mathcal{F}(X,R)$ も可換環である．

特に $\mathcal{F}(\mathbb{R},\mathbb{R})$ には $\mathbb{R}$ 上定義された連続関数や微分可能関数が含まれている．

問 2.1.6 $\mathcal{F}(\mathbb{R},\mathbb{R})$ は整域か？　整域であるなら証明せよ．また，整域でないなら反例を挙げよ．

例 2.1.9 $\mathcal{C}(\mathbb{R},\mathbb{R}),\mathcal{D}(\mathbb{R},\mathbb{R})$ で，それぞれ $\mathbb{R}$ 上の実数値連続関数，微分可能関数の全体を表す．すると $\mathcal{D}(\mathbb{R},\mathbb{R})$ は $\mathcal{C}(\mathbb{R},\mathbb{R})$ の部分環であり，$\mathcal{C}(\mathbb{R},\mathbb{R})$ は $\mathcal{F}(\mathbb{R},\mathbb{R})$ の部分環である．

定義 2.1.7 $R_1,\cdots,R_n$ を n 個の環とする．直積集合

$$R:=\prod_{i=1}^{n}R_i=R_1\times\cdots\times R_n$$

の二元 $(x_1,\cdots,x_n),(y_1,\cdots,y_n)$ に対し，それらの和と積を

$$(x_1+y_1,\cdots,x_n+y_n),\quad (x_1y_1,\cdots,x_ny_n)$$

により定める．すると R は環をなす．これを環 $R_1,\cdots,R_n$ の **直積** という．$(0,\cdots,0)$ が零元であり，$(1,\cdots,1)$ が単位元である．

次の性質は，定義から直ちに得られる：

補題 2.1.8 R を環とし，$a,b,c\in R$ とするとき，次が成り立つ：

(1) $-0=0$,

(2) $a0=0a=0$,

(3) $-(ab)=(-a)b=a(-b)$,

(4) $-(-a)=a$,

(5) $(-a)(-b)=ab$,

(6) $a(b-c)=ab-ac$, $(a-b)c=ac-bc$.

問 2.1.9 上の補題を証明せよ．

2.1.2 環の単数群と体

定義 2.1.10 R の元 u が, 乗法に関して逆元を持つとき, 即ち,

$$uv = vu = 1 \quad (\exists v \in R)$$

となるとき, u を R の **単数** といい, その全体を $R^\times$ と表す. R に於ける積は, 二項演算

$$\times : R^\times \times R^\times \longrightarrow R^\times$$

を導き, $(R^\times; \times)$ は群をなす. この群を, $U(R)$, または, $R^\times$ と表し, 環 R の **単数群** または **乗法群** という.

問 2.1.11 $R^\times$ が群をなすことを確かめよ.

定義 2.1.12 $R^\times = R - \{0\}$ となる環 R を **斜体**という. (乗法に関して) 可換な斜体を **体** という.

問 2.1.13 体は整域であることを確かめよ.

定義 2.1.14 (斜) 体 K の部分集合 k が部分環であって, k の 0 以外の元が (乗法に関する) 逆元をもつとき, k を K の **部分 (斜) 体** という.

例 2.1.10 $\mathbb{Q}$, R, C は, 通常の和と積に関して, 体をなす. それぞれ, **有理数体**, **実数体**, **複素数体** という. $\mathbb{Q}$ は $\mathbb{R}$, $\mathbb{C}$ の部分体であり, $\mathbb{R}$ は $\mathbb{C}$ の部分体である.

問 2.1.15 $m(\neq 1)$ を平方因子 [2] を含まない整数とするとき, $\mathbb{Q}[\sqrt{m}] = \{x + y\sqrt{m} \mid x, y \in \mathbb{Q}\}$ は, 複素数体 $\mathbb{C}$ の部分体であることを示せ.

例 2.1.11 R を可換環とする. R 上の行列環の単数群 $\mathrm{M}_n(R)^\times$ を $\mathrm{GL}_n(R)$ と表し, R 上の n **次一般線形群** という:

$$\mathrm{GL}_n(R) = \{A \in \mathrm{M}_n(R) \mid \det(A)^{3}.$$

例 2.1.12 V を複素数体上の線形空間とする. V の自己準同型環 $\mathrm{End}(V)$ の単数群を, $\mathrm{GL}(V)$ と表す:

$$\mathrm{GL}(V) = \{f \in \mathrm{End}(V) \mid f \text{ は線形同型写像 }\}.$$

問 2.1.16 R_1, R_2 を環とし, $R_1^\times \times R_2^\times \subset R_1 \times R_2$ と見なすとき,

$$(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$$

が成り立つことを示せ.

---

[2] $d^2 | m$ となる 1 より大きい整数 d を m の平方因子という

[3] R を可換環とする. 行列 $M = (a_{ij}) \in \mathrm{M}_n(R)$ に対し, M の行列式を

$$\det(M) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\,\sigma(1)} \cdots a_{n\,\sigma(n)}$$

と定める. 既に学んだ行列式の多くの性質は, R が可換環の場合にも, 成り立つ.

2.2 イデアルと剰余環

2.2.1 イデアル

定義 2.2.1 環 R の加法に関する部分群 I は

$$a \in R,\, x \in I \Longrightarrow ax \ \in I$$

を満たすとき, **左イデアル** と呼ばれる. また,

$$a \in R,\, x \in I \Longrightarrow xa \ \in I$$

を満たすとき, **右イデアル** と呼ばれる. 左イデアルであり, 同時に右イデアルでもあるとき, **両側イデアル**, 或いは単に, **イデアル** という. R が可換環ならば, これらの区別は必要でない.

例 2.2.1 環 R に於いて, $R, \{0\}$ は両側イデアルである. R を **単位イデアル** といい, $\{0\}$ を **零イデアル** という.

問 2.2.2 体 F のイデアルは, F と $\{0\}$ に限ることを示せ.

注意 2.2.1 直積環 $R = R_1 \times \cdots \times R_n$ の部分集合

$$\{0\} \times \cdots \times \{0\} \times R_i \times \{0\} \times \cdots \times \{0\}$$

は, R のイデアルであるが, 部分環ではない.

定義より, 次を得る:

補題 2.2.3 R を環とし, $\mathcal{I} = \{I_\lambda \mid \lambda \in \Lambda\}$ を左（右, 両側）イデアルの集合とする. このとき,

$$\bigcap_{\lambda \in \Lambda} I_\lambda$$

は, 左（右, 両側）イデアルである.

例 2.2.2 環 R の部分集合 X に対し, X を含む最小の左イデアル, 右イデアルは,

$$RX := \{\sum\ a_i x_i \mid a_i \in R, x_i \in X\}, \quad XR := \{\sum\ x_i a_i \mid a_i \in R, x_i \in X\} \quad \text{（和は有限和）}$$

と表され, X の**生成する** 左イデアル, 右イデアルという. X を含む最小の（両側）イデアルは

$$RXR := \{\sum\ a_i x_i b_i \mid a_i, b_i \in R, x_i \in X\} \quad \text{（和は有限和）}$$

と表され, X の**生成する** （両側）イデアルという. X が有限集合のとき, RX, XR, RXR は, **有限生成** 左（右, 両側）イデアルという. $X = \{x\}$ のとき, **単項** 左（右, 両側） **イデアル** という.
$X = \{x_1, \cdots, x_n\}$ のとき, X の生成する両側イデアルを $(x_1, \cdots, x_n)$ と表す.

有理整数環のイデアルは, 特別な性質を持つ.

補題 2.2.4 I を有理整数環 $\mathbb{Z}$ の部分集合とする．このとき, 次は同値である．

(1) I は, 有理整数環 $\mathbb{Z}$ のイデアルである．

(2) I は, 加法群 $\mathbb{Z}^+$ の部分群である．

証明　(1) $\Longrightarrow$ (2) は定義より明らか．I を $\mathbb{Z}^+$ の部分群とすれば, $n \in \mathbb{Z}$ と $x \in I$ との積は,

$$nx = \begin{cases} \overbrace{x + \cdots + x}^{n} & (n > 0), \\ 0 & (n = 0), \\ \overbrace{(-x) + \cdots + (-x)}^{-n} & (n < 0) \end{cases}$$

と表される．従って, I は部分群なので, $nx \in I$．よって, I はイデアルである．　□

全てのイデアルが単項である環（整域）を **単項イデアル環（整域）** という．

問 2.2.5 R を整域とする．このとき次を証明せよ．
$a, b \in R$ に対し, $a = ub$ となる単数 u が存在することは, $(a) = (b)$ で有る為の必要十分条件である．

補題 2.2.6 有理整数環 $\mathbb{Z}$ のイデアル I は, 非負整数 m が一意的に定まり, $I = (m)$ と表される．特に, $\mathbb{Z}$ は単項イデアル整域である．

証明　$\mathbb{Z}$ が整域であることは良い．I を $\mathbb{Z}$ のイデアルとする．$I = \{0\}$ のとき, $I = (0)$．$I \neq (0)$ とすると, $a \in I$ となる整数 a が存在する．このとき, $-a \in I$ なので, I は正整数を含む．I に含まれる最小の正整数を m とするとき, $I = (m)$ である．実際, $(m) \subseteq I$ は明らかである．また, $a \in I$ とし, a を m で割った商を q, 余りを r とする:

$$a = qm + r \quad (r < m).$$

このとき, $r = a - qm \in I$．m の取り方より, $r = 0$ となり, $a = qm \in (m)$．従って, $I = (m)$．　□

例 2.2.3 $\mathrm{M}_n(R)$ を環 R 上の行列環とする．(i, j) 成分が 1 で他の成分が全て 0 の行列を e_{ij} と表し, **行列単位** という．

$$J_j = \mathrm{M}_n(R)e_{ij}$$

は, j 列以外の成分がすべて 0 となる行列全体のなす左イデアルであり,

$$I_i = e_{ij}\mathrm{M}_n(R)$$

は, i 行以外の成分がすべて 0 となる行列全体のなす右イデアルである．また,

$$\mathrm{M}_n(R) = \mathrm{M}_n(R)e_{ij}\mathrm{M}_n(R)$$

が成り立つ．

問 2.2.7 上の例を確かめよ.

注意 2.2.2 以後、煩雑なので, 左イデアルについて議論を進める. 右イデアル, イデアルについても, 同様な議論が成り立つことに注意する.

イデアルの和集合は, 一般には, イデアルにならないが, 特別な場合はイデアルになることがある:

補題 2.2.8 R を環とし, $\mathcal{I} = \{I_\lambda \mid \lambda \in \Lambda\}$ を左イデアルの集合とする. 任意の $\lambda, \mu \in \Lambda$ に対し, ある $\nu \in \Lambda$ が存在して $I_\lambda \subseteq I_\nu, I_\mu \subseteq I_\nu$ を満たすとする. このとき,

$$I := \bigcup_{\lambda \in \Lambda}^{\infty} I_\lambda$$

は, R の左イデアルである.

問 2.2.9 上の補題を証明せよ.

定義 2.2.10 R を環とする. $I_1, \cdots, I_n$ を R の左イデアルとする. このとき, 左イデアル

$$I_1 + \cdots + I_n = \{\sum_{i=1}^{n} x_i \mid x_i \in I_i \ (i = 1, \cdots, n)\}$$

を, $I_1, \cdots, I_n$ の **和** という.

R のイデアル I, J に対し, イデアル

$$IJ = \{\sum_{i} x_i y_i \mid x_i \in I, y_i \in J\} \quad \text{（和は有限和）}$$

を, イデアル I, J の **積** という.

補題 2.2.11 I, J を R のイデアルとするとき, $IJ \subseteq I \cap J$ が成り立つ.

R が可換環で, $R = I + J$ ならば, $IJ = I \cap J$ が成り立つ.

証明 I, J は左イデアルなので,

$$IJ \subseteq IR \subseteq I, \quad IJ \subseteq RJ \subseteq J$$

であり, $IJ \subseteq I \cap J$.

R は可換環とする. $R = I + J$ とすれば, $1 = x + y \quad (\exists x \in I, \ \exists y \in J)$ が成り立つ. 任意の $a \in I \cap J$ に対し, $a = a(x + y) = ax + ay \in JI + IJ = IJ$ が成り立ち, $I \cap J \subseteq IJ$ を得る. 従って, $IJ = I \cap J$ を得る. □

2.2.2 剰余環

定義 2.2.12 I を環 R のイデアルとする. $x, y \in R$ に対し, $x - y \in I$ のとき,

$$x \equiv y \pmod{I}$$

と表し, x と y は, I を **法として合同** という. この関係は同値関係をなす. $x \in I$ に対し, x を含む同値類を $[x]_I$, 或いは, 単に, $[x]$ と表す.

問 2.2.13 I を法として合同であるという関係は, 同値関係であることを確かめよ.

定理 2.2.14 R を環, $I\ (\subsetneq R)$ をイデアルとし, R/I をアーベル群としての剰余群とする. このとき, $x, y \in R$ に対し, xy を含む剰余類 $[xy]$ は x, y の取り方によらず $[x], [y]$ にのみ依存する. 更に, 二項演算

$$\times : R/I \times R/I \longrightarrow R/I, \quad ([x], [y]) \longmapsto [xy]$$

に対し, $(R/I; +, \times)$ は $[0]$ を零元, $[1]$ を単位元とする環をなす. R が可換環ならば, R/I も可換環である.

証明 $I \subsetneq R$ なので, $[1] \neq [0]$ に注意する. $x - x', y - y' \in I$ ならば, I はイデアルなので, $xy - xy' \in I$ となり, 前半を得る. 積に関する結合法則は,

$$[x]([y][z]) = [x][yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z].$$

証明の残りは, 演習問題とする. □

問 2.2.15 定理の証明を完成させよ.

定義 2.2.16 環 $(R/I; +, \times)$ を R の I に関する **剰余環** といい, 単に, R/I と表す.

例 2.2.4 m を 2 以上の整数とする. このとき $\mathbb{Z}/(m) = \{[0], [1], \cdots, [m-1]\}$ であり, $[r]$ は m で割ると剰余が r となる整数全体の集合である. これが剰余類の名称の由来となっている.

例 2.2.5 $\mathbb{Z}$ 有理整数環とし, $m\ (\geq 2)$ を自然数とする. 剰余環 $\mathbb{Z}/(m)$ の単数群 $(\mathbb{Z}/(m))^\times$ を, m に関する **既約剰余類群** という. その位数は, $|(\mathbb{Z}/(m))^\times| = \varphi(m)$ を満たす. 但し, φ は Euler の関数 [4] である.

2.3 環射

2.3.1 環射の定義と例

定義 2.3.1 環 R から環 R' への写像

$$f : R \longrightarrow R'$$

は, 次を満たすとき, **環準同型写像**, 或いは, **環射** と呼ばれる.

(RH1) $f(x + y) = f(x) + f(y) \quad (\forall x, y \in R)$,

(RH2) $f(xy) = f(x)f(y) \quad (\forall x, y \in R)$,

(RH3) $f(1) = 1$.

環射 $f : R \longrightarrow R'$ は, 積を無視すると, 群射 $f : R^+ \longrightarrow R'^+$ である. 従って $f(0) = 0$ である. しかし, $f(1) = 1$ は, (RH2) から得られるとは限らない.

[4] m を自然数とし, $1, 2, \cdots, m$ の内, m と互いに素なものの個数を $\varphi(m)$ と表す. $varphi$ を **Euler の関数**という.

定義 2.3.2 集合の写像として全単射である環射を, **環同型射** という. R から R' への環同型射が存在するとき, R と R' は **同型** であるといい

$$R \simeq R'$$

と表す.

R, R' が体のとき, 環同型射 $f; R \longrightarrow R'$ を **体同型射** という.

例 2.3.1 V を複素数体上の n 次元線形空間とし, $(v_1, \cdots, v_n)$ を順序づけられた V の基底とする. 各線形写像 $f \in \mathrm{End}_{\mathbb{C}}(V)$ に対し, 行列 $M(f) \in \mathrm{M}_n(\mathbb{C})$ を,

$$(f(v_1), \cdots, f(v_n)) = (v_1, \cdots, v_n)M(f)$$

により定める. このとき,

$$\Phi : \mathrm{End}_{\mathbb{C}}(V) \longrightarrow \mathrm{M}_n(\mathbb{C})$$

は, 環同型射である.

例 2.3.2 写像

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad n \longmapsto 2n$$

は, $f(1) = 2 \neq 1$ なので環射ではない.

例 2.3.3 R を環とし, S をその部分環とする. このとき,

$$\iota : S \longrightarrow R, \quad y \longmapsto y$$

は環単射（$1:1$ の環射）となる. これを **自然な環単射** と名付ける.

例 2.3.4 $f : R \longrightarrow R'$ を環単射とするとき, $f(R)$ は R' の部分環である. このとき, R と $f(R)$ を同一視し, R を R' の部分環と見なす. 例えば,

$$\iota : \mathbb{C} \longrightarrow \mathrm{M}_2(R), \quad a + bi \longmapsto aI_2 + bJ_2$$

は環単射である, 但し,

$$J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

従って, $\mathbb{C} = \{aI_2 + bJ_2 \mid a, b \in \mathbb{R}\}$ と見なせる.

補題 2.3.3 $f : R \longrightarrow R'$ を環射とする. I' が R' のイデアルならば, $f^{-1}(I')$ は R のイデアルである. 特に, $f^{-1}(0)$ は R のイデアルである.

問 2.3.4 上の補題を証明せよ.

定義 2.3.5 環射 $f : R \longrightarrow R'$ に対し, イデアル $f^{-1}(0)$ を f の **核** といい, $\mathrm{Ker}(f)$ と表す.

補題 2.3.6 $f : R \longrightarrow R'$ を環射とする. $\mathrm{Ker}(f) = (0)$ は, f が単射である為の必要かつ十分な条件である.

証明　$f(x) = f(y)$ とすると, $f(x-y) = f(x) - f(y) = 0$. $\mathrm{Ker}(f) = (0)$ ならば, $x - y = 0$ となり 1, $x = y$. 従って, f は単射である. 逆に, f を単射と仮定する. $x \in \mathrm{Ker}(f)$ とすると, $f(x) = 0 = f(0)$. f は単射なので, $x = 0$. 従って, $\mathrm{Ker}(f) = (0)$. □

補題 2.3.7　$f : k \longrightarrow R$ を体 k から環 R への環射とする. このとき f は単射である.

証明　$\mathrm{Ker}(f)$ は k のイデアルである. 体 k のイデアルは, $\{0\}$ と k のみであり, $1 \notin \mathrm{Ker}(f)$ なので, $\mathrm{Ker}(f) \neq k$. 従って, $\mathrm{Ker}(f) = \{0\}$. よって f は単射である. □

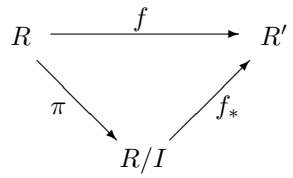
例 2.3.5　I を環 R のイデアル（$I \neq R$）とする.

$$\pi : R \longrightarrow R/I, \quad x \longmapsto [x]$$

は環全射であり, $\mathrm{Ker}(\pi) = I$ をみたす. π を **自然な環全射** という. I を含むイデアル J に対し, R/I のイデアル $\pi(J)$ を J/I と表す.

2.3.2　同型定理

定理 2.3.8　（環射の分解定理）$f : R \longrightarrow R'$ を環射とし, $I = \mathrm{Ker}(f)$ とする. このとき, 環単射 $f_* : R/I \longrightarrow R'$ で $f_* \circ \pi = f$ を満たすものが唯一つ存在する：



ただし $\pi : R \longrightarrow R/I$ は自然な環全射である. 特に, $R/I \simeq f(R) = f_*(R/I)$.

証明　$x, y \in R$ は, $x \equiv y \pmod{I}$ を満たすとすると, $x - y \in I = \mathrm{Ker}(f)$. 従って, $f(x-y) = 0$ となり, $f(x) = f(y)$. よって,

$$f_* : R/I \longrightarrow R', \quad [x] \longmapsto f(x)$$

は, $[x]$ の代表元の取り方に依らず, 写像である. f が環射なので, f_* も環射であり, 定義より, $f_* \circ \pi = f$.

$[x] \in \mathrm{Ker}(f_*)$ ならば, $f_*([x]) = f(x) = 0$. 従って, $x \in \mathrm{Ker}(f) = I$ となり, $[x] = 0$. よって, f_* は単射である. □

系 2.3.9　（環同型定理）$f : R \longrightarrow R'$ を環全射とするとき,

$$R/\mathrm{Ker}(f) \simeq R.$$

証明　$f_* : R/\mathrm{Ker}(f) \longrightarrow R$ は, 定理により, 環単射であり, $R' = f(R) = f_*(R/\mathrm{Ker}(f))$ なので, 全射である. □

定理 2.3.10 （対応定理）R を環とし, I $(\neq R)$ をイデアルとする. I を含む R のイデアル全体のなす集合 $\mathcal{I}$ と, R/I のイデアル全体のなす集合 $\bar{\mathcal{I}}$ は,

$$\Phi : \mathcal{I} \longrightarrow \bar{\mathcal{I}}, \quad J \longmapsto \pi(J)$$

により, 一対一に対応する.

証明 写像 $\Psi : \bar{\mathcal{I}} \longrightarrow \mathcal{I}$ を $\Psi(\bar{J}) = \pi^{-1}(\bar{J})$ により定める. このとき, Φ と Ψ は互いに他の逆写像であり, 結論を得る. □

問 2.3.11 Φ と Ψ が互いに他の逆写像であることを確かめよ.

例 2.3.6 R を環とする. $n \in \mathbb{Z}$ に対し, 1 の n 倍を次のように定める.

$$n \cdot 1 \ {}^{5} := \begin{cases} \overbrace{1+1+\cdots+1}^{n\text{ 個}} & (n > 0) \\ 0 & (n = 0) \\ \overbrace{1+1+\cdots+1}^{-n\text{ 個}} & (n < 0) \end{cases} \tag{2.1}$$

写像

$$\phi : \mathbb{Z} \longrightarrow R, \quad n \longmapsto n \cdot 1$$

は環射である. この様に, 有理整数環からすべての環への「自然な」環射が存在する.

像 $\phi(\mathbb{Z})$ は, R の部分環であり, 同形定理により

$$\mathbb{Z}/\mathrm{Ker}(\phi) \simeq \phi(\mathbb{Z}) \subseteq R.$$

$\mathbb{Z}$ のイデアルは, 補題 2.2.6 により, 単項イデアルなので, $\mathrm{Ker}(\phi) = (m)$ となる $0 \leq m \ (\neq 1) \in \mathbb{Z}$ が, 一意的に, 存在する. m を 環 R の **標数** といい, $\mathrm{char(R)}$ と表す.

例えば,

$$\mathrm{char}(\mathbb{Z}) = 0, \quad \mathrm{char}(\mathbb{Q}) = 0, \quad \mathrm{char}(\mathbb{C}) = 0, \quad \mathrm{char}(\mathbb{Z}/(m)) = m \ (1 < m \in \mathbb{Z}).$$

標数 0 の環は, $\mathbb{Z}$ と同型な環を含むので, 無限環（無限個の要素を持つ環）である. 従って有限環の標数は 2 以上の整数である.

2.3.3 中国剰余定理

この小節では, 環は全て可換環とする.

定義 2.3.12 R を可換環とし, $x, y \in R$ とする. 有理整数環における倍数の概念を拡張して, $(x) \subseteq (y)$ のとき, x は, y の **倍数**, また, y は x の **約数** といい, $y|x$ と表す. 公約数, 最大公約数, 公倍数, 最小公倍数も（有理）整数の場合と同様に定義される.

また, $(a) + (b) = R$ となるとき, 即ち, $ax + by = 1$ を満たす $x, y \in R$ が存在するとき, a と b とは, **互いに素である** といい, $(a, b) = 1$ と表す.

[5] 整数が環 R には含まれているとは限らないので, (2.1) は, 整数 n と R の元 1 との積ではないことに注意する.

定理 2.3.13（中国剰余定理）$m_1, \cdots, m_r$ を

$$(m_i, m_j) = 1 \ \ (i \neq j)$$

を満たす自然数とする．この時与えられた整数 $a_1, \cdots, a_r$ に対し，

$$a \equiv a_i \pmod{m_i},\ 1 \leq i \leq r$$

を満たす整数 a が存在する．

証明　$M_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_n$ とすると，M_i と m_i は互いに素である．従って

$$M_i t_i \equiv 1 \pmod{m_i}, \quad i = 1, \cdots, n$$

を満たす整数 t_i が存在する．このとき

$$x = a_1 M_1 t_1 + \cdots + a_n M_n t_n$$

が求める解である．　□

例 2.3.7

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}. \quad x \equiv 2 \pmod{7}$$

を満たす最小の正整数を求めよう．

このような問題の解法は，中国において古くから知られていたのである．上の問題の解法を，次の漢詩（程大位：算法統宗（1593），cf. [?]）が示している．

三 人 同 行 七 十 稀
五 樹 梅 花 廿 一 枝
七 子 團 円 正 半 月
除 百 零 五 便 得 知

$M_1 = 35.\ M_2 = 21,\ M_3 = 15$ とおく．次の部分が漢詩の一句，二句，三句である：

$$70 \equiv 1 \pmod{3}, \quad 21 \equiv 1 \pmod{5}, \quad 15 \equiv 1 \pmod{7}.$$

従って

$$t_1 = 2, \quad t_2 = 1, \quad t_3 = 1$$

であり，次が四句である：

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233, \quad x = 233 - 2 \cdot 105 = 23.$$

すなわち最小の正整数解は $x = 23$ である．

中国剰余定理を一般の可換環に拡張しよう．

補題 2.3.14 R を可換環とし, $I, I_1, \cdots, I_n$ を R のイデアルとする. $R = I + I_j$ $(\forall j)$ とすると

$$R = I + I_1 \cdots I_n = I + (I_1 \cap \cdots \cap I_n).$$

証明 補題 2.2.11 を繰り返し用いて

$$I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$$

を得る. 従って

$$I + I_1 \cdots I_n \subset I + (I_1 \cap \cdots \cap I_n) \subseteq R.$$

仮定より, 各 i に対し

$$1 = x_i + y_i \quad (\exists x_i \in I,\ \exists y_i \in I_i).$$

このとき

$$\prod_{i=1}^{n} y_i = \prod_{i=1}^{n} (1 - x_i) = 1 + x \quad (\exists x \in I).$$

従って

$$1 = -x + y_1 \cdots y_n \in I + (I_1 \cap \cdots \cap I_n).$$

よって $R \subseteq I + I_1 \cdots I_n$ となる. □

補題 2.3.15 R を可換環とし, $I_1, \cdots, I_n$ を R のイデアルとする. $R = I_i + I_j$ $(1 \leq i < j \leq n)$ ならば

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

証明 補題 2.2.11 を繰り返し用いて

$$I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$$

を得る. 逆の包含関係を n に関する帰納法で示す. $n = 2$ のときは, 補題 2.2.11. そこで, $n - 1$ のとき正しいとする. 前補題により, $I_1 \cdots I_{n-1} + I_n = R$ を得るので, $n = 2$ のときから

$$(I_1 \cap \cdots \cap I_{n-1}) \cap I_n \subseteq (I_1 \cdots I_{n-1}) \cap I_n \subseteq I_1 \cdots I_n$$

を得る. □

定理 2.3.16 （中国剰余定理） $I_1, \cdots, I_n$ を可換環 R のイデアルで

$$I_k + I_l = R, \quad 1 \leq k \neq l \leq n$$

を満たすとする. このとき, 次が成り立つ:

(1)

$$I_k + \cap_{l \neq k} I_l = R \quad (1 \leq \forall k 1 \leq n).$$

(2) 写像

$$f : R \longrightarrow R/I_1 \times \cdots \times R/I_n, \quad x \longmapsto (x + I_1, \cdots, x + I_n)$$

は環全射である.

(3)
$$\mathrm{Ker}(f) = \cap_{k=1}^{n} I_k = I_1 \cdots I_n.$$

証明 (1) 補題 2.3.14 より直ちに得られる.
(2) 写像 f は, 明らかに環射であり, その核は, $\mathrm{Ker}(f) = I_1 \cap \cdots \cap I_n$. f が全射であることを示そう. (1) により, 各 k に対し, $1 = x_k + y_k$ $(x_k \in I_k,\ y_k \in \cap_{l \neq k} I_l)$ と表される. 任意の $a_1, \cdots, a_n \in R$ に対し, $x = a_1 y_1 + \cdots + a_n y_n$ とするとき,

$$x - a_k = \sum_{l \neq k} a_l y_l + a_k(x_k - 1) = \sum_{l \neq k} a_l y_l - a_k y_k.$$

$l \neq k$ ならば, $y_l \in I_k$ なので, $x - a_k \in I_k$. 従って,

$$f(x) = (x + I_1, \cdots, x + I_n) = (a_1 + I_1, \cdots, a_n + I_n)$$

となり, f は全射である.
(3) 補題 2.3.15 より, $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ を得る. □

例 2.3.8 m を 2 以上の整数とし
$$m = p_1^{e_1} \cdots p_n^{e_n}$$
をその素因数分解とする. $i \neq j$ ならば $p_i^{e_i}$ と $p_j^{e_j}$ とは互に素なので
$$1 = x p_i^{e_i} + y p_j^{e_j}$$
となる整数 x, y が存在する. 即ち
$$\mathbb{Z} = (p_i^{e_i}) + (p_j^{e_j}).$$

従って, 中国剰余定理より
$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}.$$
この写像を単数群に制限して群同型射
$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_n^{e_n}\mathbb{Z})^\times$$
を得る. 両辺の位数を比べて
$$\varphi(m) = \prod_{i=1}^{n} \varphi(p_i^{e_i}) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1) = m \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right).$$

2.4 多項式環

2.4.1 一変数冪級数環と多項式環の定義

二つの整式の和と積に就いて, 読者諸賢は既に承知していることであろうが, この小節では, それらを少し異なった観点から定義してみよう.

負でない整数の集合 $\mathbb{N}_0$ は, 加法に関して, 単位半群をなす. $\mathbb{N}_0$ から環 R への写像の全体のなす集合を $\mathcal{F}(\mathbb{N}_0, R)$ と表す. 写像 $f \in \mathcal{F}(\mathbb{N}_0, R)$ は, $f(-m) = 0$ $(m < 0)$ と定義することで, $\mathbb{Z}$ から R への写像と見なせる.

$f, g \in \mathcal{F}(\mathbb{N}_0, R)$ の和と積を

$$(f+g)(n) = f(n) + g(n), \quad (f \cdot g)(n) = \sum_{m=0}^{n} f(m)g(n-m) \quad (\forall n \in \mathbb{N}_0)$$

により定めると, $(\mathcal{F}(\mathbb{N}_0, R); +, \cdot)$ は環をなす. この環は, 例 2.1.8 で定義した環と積の定め方が異なることに注意する.

例えば, 積に関する結合法則を確かめてみよう：$f, g, h \in \mathcal{F}(\mathbb{N}_0, R)$ と任意の $n \in \mathbb{N}_0$ に対し, $g(-m) = 0$ $(m < 0)$ に注意すると, 次を得る：

$$\begin{aligned}
(f(gh))(n) &= \sum_{m=0}^{n} f(m)(gh)(n-m) \\
&= \sum_{m=0}^{n} f(m)(\sum_{l=0}^{n-m} g(l))h(n-m-l)) \\
&= \sum_{m=0}^{n} f(m)(\sum_{L=m}^{n} g(L-m))h(n-L)) \\
&= \sum_{m=0}^{n} f(m)(\sum_{L=0}^{n} g(L-m))h(n-L)) \\
&= \sum_{L=0}^{n}(\sum_{m=0}^{n} f(m)g(L-m))h(n-L) \\
&= \sum_{L=0}^{n}(fg)(L)h(n-L) = ((fg)h)(n).
\end{aligned}$$

従って, $f(gh) = (fg)h$ が成り立つ.

さて, 写像 $f : \mathbb{N}_0 \longrightarrow R$ は, R の元の列

$$(f(0), f(1), \cdots, f(n), \cdots)$$

と同一視される. 更に, X を文字とするとき, f は, 形式的な無限和

$$f(X) = \sum_{n=0}^{\infty} f(n)X^n$$

と同一視される. $f(X)$ を, f に付随する, R **係数一変数形式的冪級数** と呼び, $f(n)$ を $f(X)$ の n 次係数という. これら冪級数の和と積を対応する写像の和と積により定めることで, R 係数一変数形式的冪級数の全体のなす集合 $R[[X]]$ は, $(\mathcal{F}(\mathbb{N}_0, R); +, \times)$ と同一視され, 環をなし, R **係数一変数形式的冪級数環** と呼ばれる. R が可換環ならば, $R[[X]]$ も可換環である.

R の元 a と形式的冪級数

$$a + 0X + 0X^2 + \cdots + 0X^n + \cdots$$

を同一視すると, R は $R[[X]]$ の部分環をなし,

$$r(fg) = (rf)g = f(rg) \quad (\forall r \in R,\ \forall f, g \in R[[X]])$$

を満たす.

有限個の係数のみが 0 でない, 即ち, $\{n \in \mathbb{N}_0 \mid f(n) \neq 0\}$ が有限集合となる形式的冪級数 $f(X)$ を R **係数一変数多項式** という. R 係数一変数多項式の全体 $R[X]$ は, $R[[X]]$ の部分環をなし, R **係数一変数多項式環** と呼ばれる.

多項式 $f(X) \in R[X]$ は, $f(m) = 0$ $(\forall m > n)$ となる n が存在するので,

$$f(X) = a_0 + a_1X + \cdots + a_nX^n + 0X^{n+1} + \cdots$$

と表される. このとき,

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

と略記する. $a_n \neq 0$ のとき, n を $f(X)$ の **次数** といい, $\deg(f(X)) = n$ と表す. また, 多項式 0 の次数は ∞ とする.

例 2.4.1 R を整域とするとき

$$(R[X])^\times = R^\times.$$

R が整域でないとき, これは正しくない. 例えば $(\mathbb{Z}/(9))[X]$ に於いて, $[1] + [3]X$ は, $([1] + [3]X)([1] - [3]X) = [1]$ なので, 単数である.

2.4.2 多項式環の基本的性質

この小節では, R は可換環とする.

命題 2.4.1 $f(X), g(X) \in R[X]$ とする.

(1) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

(2) R が整域ならば,

$$\deg(fg) = \deg(f) + \deg(g).$$

特に, $R[X]$ も整域である.

証明 (1) は明らかなので, (2) を示す.

$$\begin{aligned} f(X) &= a_nX^n + \cdots + a_1X + a_0 \quad (a_n \neq 0) \\ g(X) &= b_mX^m + \cdots + b_1X + b_0 \quad (b_m \neq 0) \end{aligned}$$

とする. このとき, $n = \deg(f), m = \deg(g)$ であり,

$$f(X)g(X) = (a_nb_m)X^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)X^{n+m-1} = \cdots + (a_1b_0 + a_0b_1)X + a_0b_0.$$

R は整域なので, $a_nb_m \neq 0$. よって,

$$\deg(fg) = n + m = \deg(f) + \deg(g)$$

が成り立つ.

$f \neq 0, g \neq 0$ ならば, $\deg(f) \neq -\infty, \deg(g) \neq -\infty$. 従って, $\deg(fg) \neq -\infty$ となり, $fg \neq 0$. よって, R は整域である. □

命題 2.4.2 （多項式の整除）$f(X), g(X) \in R[X]$ とし, g の最高次係数は R の単数とする. このとき,

$$f = qg + r, \quad \deg r < \deg g$$

を満たす $q, r \in R[X]$ が存在する.

R が整域ならば, q, r は一意的に定まる.

証明 $\deg f$ に関する帰納法で示す. $\deg f = m, \deg g = n$ とし,

$$f = a_m X^m + \cdots + a_1 X + a_0, \quad g = b_n X^n + \cdots + b_1 X + b_0$$

と表す. ここで, 仮定により, $b_n \in R^\times$. $m < n$ のときは, $q = 0, r = f$ とすれば良い. $m \geq n$ とすると, $\deg(f - a_m b_n^{-1} X^{m-n} g) \leq m - 1$. すると, 帰納法の仮定により,

$$f - a_m b_n^{-1} X^{m-n} g = q_1 g + r_1, \quad r_1 < \deg g$$

を満たす q_1, r_1 が存在する. そこで, $q = a_m b_n^{-1} X^{m-n} + q_1, r_1 = r$ とすれば良い.

R が整域とするとき, $R[X]$ も整域であり, q, r の一意性は容易に得られる. □

問 2.4.3 R が整域のとき, q, r の一意性を確かめよ.

S を R の拡大環[6] とする. 多項式 $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ と, $\alpha \in S$ に対し,

$$f(alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

を f に α を代入した値という. $f(\alpha) = 0$ となるとき, α は多項式 $f(X)$ の **根** という.

写像 $R[X] \longrightarrow S;\ f(X) \longmapsto f(\alpha)$ は環射であり, その像を $R[\alpha]$ と表す. $R[\alpha]$ は, R と α を含む, S の最小の部分環である.

系 2.4.4 （剰余の定理）$f(X) \in R[X]$ とし, $\alpha \in R$ とする. このとき,

$$f(X) = q(X)(X - \alpha) + f(\alpha)$$

を満たす $q(X) \in R[X]$ が存在する.

問 2.4.5 上の系を証明せよ.

系 2.4.6 R を整域とする. n 次多項式 $f(X) \in R[X]$ は, 高々 n 個の根を持つ.

問 2.4.7 上の系を証明せよ.

定理 2.4.8 k を体とするとき, 一変数多項式環 $k[X]$ は単項イデアル整域である.

問 2.4.9 上の定理を証明せよ.

例 2.4.2 $i \in \mathbb{C}$ を虚数単位とする. このとき, X に i を代入する環射 $f : \mathbb{R}[X] \longrightarrow \mathbb{C}$ は全射でありその核は $(X^2 + 1)$ である.

[6] R が環 S の部分環であるとき, S を R の拡大環という.

2.4.3 単位半群環と多変数多項式

G を単位半群とし, R を環とする. R の元を係数とする G の元に関する形式的な有限和

$$\sum_{g\in G} r_g g$$

を考える. 即ち, $\{g \mid r_g \neq 0\}$ は有限集合である. これらの形式的和全体集合を $R[G]$ と表す. $R[G]$ の二元の和と積を次の様に定める：

$$\begin{array}{rcl} \sum_{g\in G} r_g g + \sum_{g\in G} s_g g & = & \sum_{g\in G}(r_g + s_g)g, \\ \left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} s_g g\right) & = & \sum_{g\in G}(\sum_{h\in G} r_h s_{h^{-1}g})g. \end{array}$$

すると, $R[G]$ は環をなす. $R[G]$ を単位半群 G の R 上の **単位半群環** という. $r \in R$ と $r\cdot 1 \in R[G]$ を同一視すれば, R は $R[G]$ の部分環であり,

$$r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta) \quad (\forall r \in R,\ \forall \alpha, \beta \in R[G])$$

を満たす.

形式的な和という考えが受け入れ難い場合は, 有限個を除いて, その像が 0 となる G から R への写像 f と形式的な和 $\sum_{g\in G} f(g)g$ を同一視すればよい.

問 2.4.10 $R[G]$ が環をなすことを証明せよ.

$X_1, \cdots, X_n$ を n 個の文字とし,

$$\mathcal{X}; = \{X_1^{e_1} \cdots X_n^{e_n} \mid e_i \in \mathbb{N}_0\ (1 \leq i \leq n)\}$$

は, $1 = X_1^0 \cdots X_n^0$ を単位元とする単位半群をなす. R を環とするとき, 単位半群環 $R[\mathcal{X}]$ を $R[X_1, \cdots, X_n]$ と表し, R **係数** n **変数多項式環** といい, その元を R **係数** n **変数多項式** という. $\mathcal{X}$ と $\mathbb{N}_0$ の n 個の直積 $(\mathbb{N}_0)^n$ は同型であることに注意する.

$(e_1, \cdots, e_n) \in (\mathbb{N}_0)^n$ に対し, 多項式

$$aX_1^{e_1} \cdots X_n^{e_n} \quad (a \in R)$$

を **単項式** という. 一般の多項式は, 単項式の **有限個** の和として表される.

$1 \leq i \leq n$ に対し, $R[X_1, \cdots, X_i]$ は $R[X_1, \cdots, X_n]$ の部分環であり, n 変数多項式を X_n に関して降冪の順に書き表すことにより, 次の同一視を得る:

$$R[X_1, \cdots, X_n] = R[X_1, \cdots, X_{n-1}][X_n].$$

0 以外の多項式

$$f(X_1, \cdots, X_n) = \sum_{(e_1, \cdots, e_n)} a_{e_1, \cdots, e_n} X_1^{e_1} \cdots X_n^{e_n} \in R[X_1, \cdots, X_n]$$

に対し

$$\deg(f) = \max\{e_1 + \cdots + e_n \mid a_{e_1,\cdots,e_n} \neq 0\}$$

を f の **次数** という. また, 多項式 0 の次数は $-\infty$ と定める.

R を環とし, $X_1, X_2, \cdots$ を文字とする. $R[X_1, \cdots, X_n] \subset R[X_1, \cdots, X_n, X_{n+1}]$ と, 自然に, 見なし,

$$R[X_1, X_2, \cdots] = \cup_{n=1}^{\infty} R[X_1, \cdots, X_n]$$

を考える. このとき, $f, g \in R[X_1, X_2, \cdots]$ に対し, n が存在し, $f, g \in R[X_1, \cdots, X_n]$ を満たす. 従って,

$$f + g,\ f \cdot g \in R[X_1, \cdots, X_n] \subset R[X_1, X_2 \cdots]$$

が定まる. このようにして, 無限個の変数を持つ多項式環 $R[X_1, X_2 \cdots]$ が定義される.

命題 2.4.11 $\phi : R \longrightarrow R'$ を環射とする. $\alpha_1, \cdots, \alpha_n \in R'$ に対し,

$$\Phi : R[X_1, \cdots, X_n] \longrightarrow R'$$

で $\Phi(X_i) = \alpha_i\ (1 \leq i \leq n)$ となるものが, 唯一つ存在する.

証明 $n = 1$ の場合を示せば, 帰納法により結論を得る. また, $n = 1$ の場合は明らかである. □

例 2.4.3 （簡約写像）R を環とし, I をそのイデアルとする.

$$R \longrightarrow A/I, \quad a \mapsto [a]$$

を標準的全とするとき, 写像

$$A[X_1, \cdots, X_n] \longrightarrow A/I[X_1, \cdots, X_n],$$

$$h = \sum a_{e_1 \cdots e_n} X_1^{e_1} \cdots X_n^{e_n} \longmapsto \bar{h} = \sum [a_{e_1 \cdots e_n}] X_1^{e_1} \cdots X_n^{e_n}$$

は環射であり, $\bar{h} = 0$ は h の係数がすべて I に含まれることを意味する. これを I に関する係数の **簡約写像** という.

R を環とする. 多項式 $f(X_1, \cdots, X_n) \in R[X_1, \cdots, X_n]$ に対し, 関数

$$\tilde{f} : R^n \longrightarrow R, \quad (a_1, \cdots, a_n) \longmapsto f(a_1, \cdots, a_n)$$

を, 多項式 f の定める **多項式関数** という.

命題 2.4.12 このとき, R が無限整域ならば,

$$\phi : R[X_1, \cdots, X_n] \longrightarrow \mathcal{F}(R^n, R), \quad f \longmapsto \tilde{f}$$

は環単射である.

証明 ϕ が環射であることは. 明らかなので, ϕ が単射であることを示そう. $\tilde{f}=0$ ならば $f=0$ であることを, n に関する帰納法で示す. $n=1$ のとき $\tilde{f}=0$ ならば, $f(a)=0$ $(\forall a\in R)$. f は多項式なので, $f\neq 0$ ならば, 系 2.4.6 より, $f(X)$ の根は有限個. そこで, $n=k$ のとき正しいとし, $n=k+1$ とする. f を X_{k+1} に関して, 降冪に展開する.

$$f(X_1,\cdots,X_{k+1})=f_mX_{k+1}^m+\cdots+f_1X_{k+1}+f_0,\quad f_m,\cdots,f_0\in K[X_1,\cdots,X_k].$$

$\tilde{f_l}=0$ $(0\leq\forall l\leq m)$ ならば, 帰納法の仮定により, $f_l=0$ $(0\leq l\leq m)$ となり, $f=0$. $\tilde{f_l}\neq 0$ $(0\leq\exists l\leq 0)$ ならば, $f_l(a_1,\cdots,a_k)\neq 0$ となる $(a_1,\cdots,a_k)\in R^k$ が存在する. このとき

$$\begin{aligned} g(X_{k+1}) &= f(a_1,\cdots,a_k,X_{k+1}) \\ &= f_m(a_1,\cdots,a_k)X_{k+1}^m+\cdots+f_1(a_1,\cdots,a_k)X_{k+1}+f_0(a_1,\cdots,a_k)\neq 0. \end{aligned}$$

$\tilde{f}=0$ なので, 一変数多項式 $g(X_{k+1})$ は $g(a_{k+1})=0$ $(\forall a_{k+1}\in R)$ を満たす. よって, $n=1$ の場合により, $g(X_{k+1})=0$. これは不合理. 従って, 命題を得る. □

2.5 可換環

この節以降, 特に断らない限り, 環は可換環とする.

2.5.1 体と極大イデアル

$\mathfrak{m}$ を環 R のイデアルで $\mathfrak{m}\neq R$ を満たすとする.

$$\mathfrak{m}\subsetneq\mathfrak{m}'\subsetneq R$$

となるイデアル $\mathfrak{m}'$ が存在しないとき, $\mathfrak{m}$ を **極大イデアル** という.

補題 2.5.1 R を可換環とし, $\mathcal{I}=\{\mathfrak{a}_\lambda\mid\lambda\in\Lambda\}$ をイデアルの集合とする. 任意の $\lambda,\mu\in\Lambda$ に対し, ある $\nu\in\Lambda$ が存在して $\mathfrak{a}_\lambda\subset\mathfrak{a}_\nu,\mathfrak{a}_\mu\subset\mathfrak{a}_\nu$ を満たすとする. このとき,

$$\mathfrak{a}:=\cup_{\lambda\in\Lambda}\mathfrak{a}_\lambda$$

は, R のイデアルである.

証明 $a,b\in\mathfrak{a}$ とすると, $a\in\mathfrak{a}_\lambda$ $(\exists\lambda\in\Lambda)$, $b\in\mathfrak{a}_\mu$ $(\exists\mu\in\Lambda)$. すると仮定により, $\mathfrak{a}_\lambda,\mathfrak{a}_\mu\subset\mathfrak{a}_\nu(\exists\nu\in\Lambda)$. 従って, $a\pm b\in\mathfrak{a}_\nu\subset\mathfrak{a}$. よって, $\mathfrak{a}$ は, R の加法群 R^+ の部分群である. また, 任意の $x\in R$ に対し, $xa\in\mathfrak{a}_\lambda\subset\mathfrak{a}$ が成り立ち, I はイデアルである. □

次の定理は, Zorn の補題の応用の恰好なものである.

定理 2.5.2 環 R のイデアル $\mathfrak{a}$ と, R の真部分集合 S が $\mathfrak{a}\cap S=\emptyset$ を満たすとする. このとき, $\mathfrak{a}$ を含み S と交わらないイデアルの中に極大なものが存在する.

証明 $\mathfrak{a}$ を含み S と交わらないイデアルの集合を $\mathcal{I}$ とする. $\mathcal{I}$ は, 包含関係により, 順序集合となり, $\mathfrak{a}$ を含むので, 空集合ではない. $\mathcal{S}$ は帰納的順序集合である. 実際 $\mathcal{T} = \{\mathfrak{a}_\lambda\}_{\lambda\in\Lambda}$ を全順序部分集合とすると,

$$\mathfrak{a}_0 = \cup_{\lambda\in\Lambda}\mathfrak{a}_\lambda$$

は, 補題 2.5.1 より, イデアルをなし, $\mathcal{T}$ の上限であることが解る. 従って, Zorn の補題により, $\mathcal{S}$ には極大元が存在する. □

系 2.5.3 （極大イデアルの存在定理）$\mathfrak{a}$ を環 R のイデアルで $\mathfrak{a} \neq R$ とする. このとき, I を含む極大イデアルが存在する.

証明 定理において, $S = \{1\}$ とすると, $\mathfrak{a}$ を含み 1 を含まない左イデアルの中に, 極大なもの $\mathfrak{m}$ が存在する. このとき, $\mathfrak{a}$ は極大

問 2.5.4 R を可換環とする. このとき, 次は同値であることを示せ.

(1) R が体である.

(2) R のイデアルは零イデアル $\{0\}$ と自分自身 R のみである.

命題 2.5.5 可換環 R のイデアル $\mathfrak{m}$ に対し次は同値である.

(1) $\mathfrak{m}$ は極大イデアルである.

(2) $R/\mathfrak{m}$ は体である.

証明 $R/\mathfrak{m}$ が体であるための必要十分条件は, 補題 2.5.4 より, $R/\mathfrak{m}$ のイデアルが $\{0\}$ と $R/\mathfrak{m}$ のみからなることである. このことは, 対応定理（定理 2.3.10 (3)） により, $\mathfrak{m}$ を含むイデアルは $\mathfrak{m}$ と R 自身であること, 即ち, $\mathfrak{m}$ が極大イデアルであることと同値である. □

例題 2.5.6 有理整数環のイデアル (p) $(p \geq 0)$ が極大イデアルである為の条件は p が素数となることである. このとき, $\mathbb{F}_p := \mathbb{Z}/(p)$ は, p 個の元からなる有限体である.

（解） (p) が極大イデアルとする. このとき, $p \neq 0$. p が素数でないとすると, $1 < a < p$ を満たす p の因数 a が存在する. すると, $(p) \subsetneq (a) \subsetneq \mathbb{Z}$ となり, 不合理である. 逆に, p が素数とする. $(p) \subsetneq (a) \subset \mathbb{Z}$ とすると, $p = ab$ を満たす $b \in \mathbb{Z}$ が存在する. p は素数なので, $a = 1$ または $a = p$. $(p) \neq (a)$ なので, $a = 1$ となり, $(a) = \mathbb{Z}$. 従って, (p) は極大イデアルである. □

例題 2.5.7 体 k の元 $a_1, \cdots, a_n$ に対し, $(X_1 - a_1, \cdots, X_n - a_n)$ は, k 上の多項式環 $k[X_1, \cdots, X_n]$ の極大イデアルであることを示せ.

（解） 環射

$$f : k[X_1, \cdots, X_n] \longrightarrow k, \quad X_i \longmapsto a_i \ (1 \leq i \leq n)$$

の核 $\mathrm{Ker}(f)$ は $(X_1 - a_1, \cdots, X_n - a_n)$ に等しい. 従って, 同型定理より,

$$k[X_1, \cdots, X_n]/(X_1 - a_1, \cdots, X_n - a_n) \simeq k.$$

よって, 命題 2.5.5 より, $(X_1 - a_1, \cdots, X_n - a_n)$ は極大イデアルである. □

2.5.2 整域と素イデアル

R を可換環とし, $a \in R$ とする.

$$ab = 0 \quad (\exists b\ (\neq 0)\ \in R)$$

のとき, a を **零因子** という. 0 以外の零因子を持たない可換環を **整域** という.

例 2.5.1 体は整域である. 整域の部分環は整域である.

例 2.5.2 $m \in \mathbb{Z}$ を合成数とするとき, $\mathbb{Z}/(m)$ は整域ではない. 例えば, $[2], [3]$ は, $\mathbb{Z}/(6)$ に於いて, 零ではないが, $[2][3] = [0]$ となる. $[2], [3] \in \mathbb{Z}/(6)$ は零因子である.

例 2.5.3 R を整域とする. $f, g \in R[X]$ に対し

$$\deg(fg) = \deg(f) + \deg(g)$$

が成立つ. このことから $R[X]$ が整域であることがわかる. 以下帰納的に $R[X_1, \cdots, X_n]$ も整域であることを知る.

例 2.5.4 R を整域とするとき

$$(R[X])^\times = R^\times.$$

R が整域でないとき, これは正しくない. 例えば $(\mathbb{Z}/(9))[X]$ に於いて, $[1] + [3]X$ は, $([1] + [3]X)([1] - [3]X) = [1]$ なので, 単数である.

可換環 R のイデアル $\mathfrak{p} \neq R$ が, $a, b \in R$ に対し

$$ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \quad \text{or} \quad b \in \mathfrak{p}$$

を満たすとき, $\mathfrak{p}$ を **素イデアル** という.

命題 2.5.8 可換環 R のイデアル $\mathfrak{p}$ に対し次は同値である.

(1) $\mathfrak{p}$ は素イデアルである.

(2) $R/\mathfrak{p}$ は整域である.

証明 (1) $\Longrightarrow$ (2) $[a][b] = [ab] = 0$ とすると, $ab \in \mathfrak{p}$. $\mathfrak{p}$ は素イデアル故, $a \in \mathfrak{p}$ 又は $b \in \mathfrak{p}$ である. 即ち, $[a] = 0$ 又は $[b] = 0$. 故に $R/\mathfrak{p}$ は整域である.
(2) $\Longrightarrow$ (1) $ab \in \mathfrak{p}$ とする. すると $[ab] = [a][b] = 0$. $R/\mathfrak{p}$ は整域なので, $[a] = 0$ 又は $[b] = 0$. 従って, $a \in \mathfrak{p}$ 又は $b \in \mathfrak{p}$ となり, $\mathfrak{p}$ は素イデアルである. □

系 2.5.9 可換環において, 極大イデアルは素イデアルである.

証明 $\mathfrak{m}$ を極大イデアルとする. 命題 2.5.5 により, $R/\mathfrak{m}$ は体である. 体は整域なので, 命題 2.5.8 により $\mathfrak{m}$ は素イデアルである. □

例 2.5.5 体 k 上の n 変数多項式環 $k[X_1, \cdots, X_n]$ において, $(X_1, \cdots, X_n)$ は極大イデアルである. しかし, $n \geq 2$ のとき, $(X_1), \cdots, (X_1, \cdots, X_{n-1})$ は素イデアルであるが, 極大イデアルではない.

例 2.5.6 $p\ (\geq 0) \in \mathbb{Z}$ とする. イデアル (p) が有理整数環 $\mathbb{Z}$ の素イデアルであるための必要十分条件は $p = 0$ であるか, または p が素数である. イデアル $\{0\}$ は素イデアルであるが, 極大イデアルではない.

例 2.5.7 R が整域ならば, R の標数 $\mathrm{char}(R)$ は 0 又は素数である.

問 2.5.10 上の例を確かめよ.

例 2.5.8 R を標数 $p > 0$ の整域とする. このとき, $p \cdot a = 0$ であり,

$$(a + b)^p = a^p + b^p$$

を満たす.

$$\sigma = \sigma_p : R \longrightarrow R, \quad a \longmapsto a^p$$

は環単射である.

ここで, 整数から有理数を構成する方法の一般化を考える.

定義 2.5.11 R を整域とし, $S = R - \{0\}$ とする. $R \times S$ の二元 $(a, s), (b, t)$ に対し

$$(a, s) \sim (b, t) \quad \Longleftrightarrow \quad at - bs = 0 \tag{2.2}$$

と定める. このとき, $\sim$ は同値関係となる. (a, s) を含む同値類を a/s と表し, 同値類の全体の集合を $Q(R)$ と表す. $a/s, b/t$ の和, 積を

$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

と定めると, これは Well-defined であり, $(Q(R)\,; +, \cdot)$ は体をなし,

$$\iota_S : R \longrightarrow Q(R), \quad a \longmapsto \frac{a}{1}$$

は環単射である. $Q(R)$ を R の **分数体**, 或いは, **商体** という. $a \in R$ と $\iota_S(a) = a/1$ を同一視すると, R は $Q(R)$ の部分環である.

例 2.5.9 有理整数環 $\mathbb{Z}$ の分数体は, 有理数体 $\mathbb{Q}$ である. 体 k 上の n 変数多項式環 $k[X_1, \cdots, X_n]$ の分数体

$$k(X_1, \cdots, X_n) = \{f(X_1, \cdots, X_n)/g(X_1, \cdots, X_n) \mid f, g \in k[X_1, \cdots, X_n]\ (g \neq 0)\}$$

を k 上の n 変数 **有理関数体** という.

定理 2.5.12 （分数体の普遍性）$f : R \longrightarrow K$ を整域 R から体 K への環単射とする. このとき f は R の分数体 $Q(R)$ から K への環単射に一意的に拡張される.

証明 記号は, 定義 2.5.11 と同じとする. f は環単射なので, $f(s) \neq 0$ $(\forall s \in S)$.

$$\Phi(a/s) := f(a)f(s)^{-1} \quad (a, s) \in R \times S$$

は, well-defined である. 実際, $(a, s) \sim (b, t)$ とするとき, $at - bs = 0$. 従って, $f(a)f(t) = f(b)f(s)$ となり,

$$\Phi(a/s) = f(a)f(s)^{-1} = f(b)f(t)^{-1} = \Phi(b/t).$$

すると, 写像 $\Phi : Q(R) \longrightarrow K$ は環単射であることが解る. 更に, Φ の一意性も明らかである. □

2.6 単項イデアル整域と一意分解整域

2.6.1 Euclid 整域と単項イデアル整域

R を整域とする. 次を満たす写像 $v : R\backslash\{0\} \rangle \mathbb{Z}$ が存在するとき, 組 (R, v) を **Euclid 整域** という.

(1) $v(a) \geq 0$.

(2) 任意の $a, b \in R$ $(a \neq 0)$ に対し

$$b = qa + r, \quad r = 0 \quad \text{または} \quad v(r) < v(a)$$

を満たす $q, r \in R$ が存在する.

v を Euclid 整域の **計量関数** という.

例 2.6.1 有理整数環 $\mathbb{Z}$, 体 k 上の一変数多項式環 $k[X]$ は Euclid 整域である. $\mathbb{Z}$ の計量関数は

$$| \ | : \mathbb{Z}\backslash\{0\} \longrightarrow \mathbb{Z}, \quad n \longmapsto |n|.$$

$k[X]$ の計量関数は

$$\deg : k[X]\backslash\{0\} \longrightarrow \mathbb{Z}, \quad f(X) \longmapsto \deg(f(X)).$$

例 2.6.2 Gauss の整数環 $\mathbb{Z}[i]$ は, ノルム写像 $\alpha \longmapsto N(\alpha) = \alpha\bar{\alpha}$ を計量関数とする Euclid 整域である. 実際, $\alpha, \beta(\neq 0)$ に対し, 複素数 α/β に最も近い $\mathbb{Z}[i]$ の元の一つを γ とする. このとき

$$\frac{\alpha}{\beta} - \gamma = a + bi, \quad |a|, |b| \leq \frac{1}{2}$$

と表される. $\beta(a + ib) = \delta$ とすれば, $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$ であり, $\delta \neq 0$ ならば

$$N(\delta) = N(\beta)(|a|^2 + |b|^2) \leq N(\beta)\frac{1}{2} < N(\beta).$$

従って $(\mathbb{Z}[i], N)$ は Euclid 整域である.

すべてのイデアルが単項イデアルである整域を **単項イデアル整域** という.

補題 2.6.1 Euclid 整域は単項イデアル整域である.

証明 $I \subseteq R$ を零イデアルと異なる任意のイデアルとする. 集合 $\{v(a) \mid a \in I - \{0\}\}$ には最小数が存在する. それを $v(a)$ とする. このとき $I \supseteq (a)$ は明らかである. 逆に $b \in I$ を任意に取れば

$$b = qa + r, \quad r = 0 \quad \text{または} \quad v(r) < v(a)$$

を満たす $q, r \in R$ が存在する. $r = b - qa \in I$ なので, a の選び方から $r = 0$ でなければならない. 従って $b = qa \in (a)$. よって $I = (a)$ となる. □

例 2.6.3 有理整数環 $\mathbb{Z}$, 体 k 上の一変数多項式環 $k[X]$, Gauss 整数環 $= Z[i]$ は単項イデアル整域である.

補題 2.6.2 単項イデアル整域 R の有限個の元 $a_1, \cdots, a_n$ $(\exists a_i \neq 0)$ に対し, これらが生成するイデアルを (d) とおく: $(a_1, \cdots, a_n) = (d)$. このとき d は $a_1, \cdots, a_n$ の最大公約数である.

証明 $a_i \in (d)$ なので, $a_i = b_i d$ $(\exists b_i \in R)$ と表される. 従って d は a_i $(i = 1, \cdots, n)$ の公約数である. また e が $a_1, \cdots, a_n$ の公約数とすると, $a_i \in (e)$ となり, $(d) = (a_1, \cdots, a_n) \subseteq (e)$ を得る. 従って $d \in (e)$ であり, e は d の約数である. よって d は $a_1, \cdots, a_n$ の最大公約数である. □

実際に, 最大公約数を求めるには, Euclid 互除法が有用である. Euclid 互除法の復習を兼ねて, 次を示そう.

補題 2.6.3 a, b, s $(s \geq 2)$ を自然数とするとき

$$(s^a - 1, s^b - 1) = s^{(a,b)} - 1.$$

証明 a, b の最大公約数を求めるために, 次のように一連の割り算を行う.

$$\begin{aligned}
a &= qb + r_1, \ \ b > r_1 > 0, \\
b &= q_1 r_1 + r_2, \ \ r_1 > r_2 > 0, \\
r_1 &= q_2 r_2 + r_3, \ \ r_2 > r_3 > 0, \\
&\cdots\cdots\cdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, \ \ r_{k-1} > r_k > 0, \\
r_{k-1} &= q_k r_k, \ \ r_{k+1} = 0.
\end{aligned}$$

このとき, $r_k = (a, b)$ である.

さて,

$$s^a - 1 = s^{qb+r_1} - s^{r_1} + s^{r_1} - 1 = s^{r_1}(s^{ab} - 1) + s^{r_1} - 1 = s^{r_1}((s^b)^{a-1} + \cdots 1)(s^b - 1) + s^{r_1} - 1$$

より, 次を満たす $Q_1, \cdots, Q_k$ が存在する.

$$\begin{aligned}
s^a - 1 &= Q(s^b - 1) + s^{r_1} - 1, \\
s^b - 1 &= Q_1(s^{r_1} - 1) + s^{r_2} - 1, \\
&\cdots\cdots\cdots \\
s^{r_{k-2}} - 1 &= Q_{k-1}(s^{r_{k-1}} - 1) + s^{r_k} - 1, \\
s^{r_{k-1}} - 1 &= Q_k(s^{r_k} - 1).
\end{aligned}$$

従って, 互除法の考え方と同様にして, 求める式を得る. □

R を整域とし $q \in R$ は 0 でも単数でもないとする.

$$q = ab \ (a, b \in R) \quad \Longrightarrow a \quad \text{or} \quad b \text{ は単数}$$

を満たすとき, q を **既約元** という. また,

$$q|ab \quad \Longrightarrow q|a \quad \text{or} \quad q|b$$

を満たすとき, q を **素元** という

定義から, 次が得られる.

補題 2.6.4 R を整域とし, $q \in R$ は 0 でも単数でもないとする. このとき次が成り立つ:

(1) q が素元であるための必要十分条件は (q) が素イデアルとなることである,

(2) q は素元ならば既約元である.

証明 (1) は定義から直ちに得られる. (2) q を素元とし, $q = ab \ (a, b \in R)$ と表す. $q|ab$ なので, $q|a$ または, $q|b$ を満たす. $q|a$ のとき, $a = qa' \ (a' \in R)$ 表され, $q = qa'b$ となる. R は整域なので, $a'b = 1$. よって, b は単数である. 同様にして, $q|b$ ならば, a が単数である. 従って, q は既約元である. □

既約元, 素元は, 共に, 素数の概念の拡張であるが, 一般には, 次の例で見るように, 既約元だからといって, 素元になるとは限らない.

例 2.6.4 $\mathbb{C}$ の部分環 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|a, b \in \mathbb{Z}\}$ において,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

と二通りに因数分解される. ここで $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ はいずれも既約元であるが素元ではない.

問 2.6.5 上の例を確かめよ.

補題 2.6.6 単項イデアル整域 R の元 $p \ (\neq 0)$ に対し, 次は同値である.

(1) p は既約元である,

(2) p は素元である,

(3) (p) は素イデアルである,

(4) (p) は極大イデアルである.

証明 (4) $\Longrightarrow$ (3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) は良い. (1) $\Longrightarrow$ (4) を示す. p を既約元とし, (p) が極大イデアルでないとする. $(p) \subsetneq (a) \subsetneq R$ を満たす $a \in R$ が存在する. すると, $p = ad \ (\exists d \in R)$ と表される. p が既約元なので, a または d は単数. d が単数ならば, $(p) = (a)$ となり不合理. a が単数ならば, $(a) = R$ となり, 不合理. 従って, (p) は極大イデアルである. □

2.6.2 一意分解整域

R を整域とし, K をその分数体とする. K の二元 a, b が R の単数倍の違いであるとき, すなわち

$$a = ub, \quad \exists u \in R^\times$$

のとき, a と b は **同伴** であるといい, $a \sim b$ と表す.

例 2.6.5 有理整数環 $\mathbb{Z}$ では, $a, b \in \mathbb{Q}$ に対し,

$$a \sim b \quad \Longleftrightarrow a = \pm b.$$

体 k 上の一変数多項式環 $k[X]$ では, $f, g \in k(X)$ に対し,

$$f \sim g \quad \Longleftrightarrow \quad f = cg \ (\exists c \in k^\times).$$

整域 R は次を満たすとき, **一意分解整域** と呼ばれる.

(UFD1) R の, 単数でなく, 0 でもない任意の元は, 既約元の積として表される.

(UFD2) $a \in R$ が

$$a = p_1 \cdots p_n, \quad a = q_1 \cdots q_m$$

と既約元の積に二通りに書けたとする. このとき, $n = m$ であり, 適当に番号を付け替えると

$$p_1 \sim q_1, \cdots, p_n \sim q_n.$$

例 2.6.6 体は一意分解整域である.

例 2.6.7 例 2.6.4 で見たように, $\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではない.

補題 2.6.7 R は (UFD1) を満たす整域とする. このとき次が成り立つ:

$$R \text{ は一意分解整域} \quad \Longleftrightarrow \quad R \text{ の既約元は素元.}$$

特に, 一意分解整域では, 既約元は素元である.

証明 ($\Longrightarrow$) R を一意分解整域とし, p をその既約元とする. $ab \in (p)$ $(a, b \in R)$ とすると, $ab = pc$ $(\exists c \in R)$ と書ける. a, b, c を既約元の積に分解する:

$$a = p_1 \cdots p_n, \quad b = p_{n+1} \cdots p_{n+m}, \quad c = q_1 \cdots q_l.$$

すると分解の一意性より, $p \sim p_i$ $(\exists i)$ となる. もし $1 \leq i \leq n$ ならば $a \in (p)$ であり, $n+1 \leq i \leq n+m$ ならば $b \in (p)$. 従って (p) は素イデアルとなり, p は素元である.
($\Longleftarrow$) $a \in R$ が

$$a = p_1 \cdots p_n, \quad a = q_1 \cdots q_m$$

と既約元の積に二通りに書けたとする. p_1 は素元なので $p_1 | q_i$ $(\exists i)$. 適当に番号を付け替えると $i = 1$ としてよい. q_1 も素元なので, $p_1 u = q_1$ となる単数 u が存在する. $q_2 u^{-1}$ を q_2 と書き換えれば

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

この操作を繰り返せば, $n = m$ であり, $p_1 \sim q_1, \cdots, p_n \sim q_n$ を得る. □

定理 2.6.8 単項イデアル整域は一意分解整域である.

証明 R を単項イデアル整域とする.

$$N = \{a \mid a \neq 0, a \notin R^{\times}, a \text{ は既約元の積として表されない }\}$$

とし, $N \neq \emptyset$ として, 矛盾を導く. $a = a_0 \in N$ とすると, a_0 は既約元ではない. 従って, 単数ではない a_0', a_1 が存在して, $a_0 = a_0' a_1$ と表される. このとき $a_0' \in N$ または $a_1 \in N$. さもなければ, a_0 は既約元の積として表されてしまう. そこで $a_1 \in N$ としてよい. すると $(a_0) \subsetneq (a_1)$. 以下同様にして, イデアルの真の増大列

$$(a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

を得る.

$$I = \cup_{i=0,1,\cdots}(a_i)$$

とすると, 補題 2.5.1 により, I はイデアルをなす. R は単項イデアル整域なので, $I = (b)$ と表され, ある i が存在して $b \in (a_i)$. このとき

$$I = (b) = (a_i) = (a_{i+1}) = \cdots .$$

これは不合理である. 従って $N = \emptyset$ が示され, (UFD1) が成り立つことが判った. (UFD2) は, 補題 2.6.6, 補題 2.6.7 を組み合わせて得られる. □

例 2.6.8 有理整数環 $\mathbb{Z}$, 体 k 上の一変数多項式環 $k[X]$, Gauss の整数環 $\mathbb{Z}[i]$ は一意分解整域である.

2.6.3 Gauss の補題とその応用

この小節では, Gauss の補題を示し, その応用として, 体 k 上の n 変数多項式環 $k[X_1, \cdots, X_n]$ が一意分解整域であることを証明する. R を一意分解整域とし, K をその分数体とする. R 係数多項式

$$f = a_n X^n + \cdots + a_1 X + a_0$$

の係数 $a_n, \cdots, a_0$ の最大公約数が 1 のとき, f を **原始多項式** という.

K 係数多項式 g $(g \neq 0) \in K[X]$ は

$$g = c \cdot g_0, \quad c \in K^{\times}, \quad g_0 \ (\in R[X]) \ : \text{原始多項式}$$

と表される. g_0 を g に付随する原始多項式という. また, c は R の単数の違いを除いて一意的に定まり, g の **内容** と呼ばれ $I(g)$ と表される.

例 2.6.9 $f = X^3 + 3X^2 + 3X + 1 \in \mathbb{Z}[X]$ は原始多項式である.

$$g = \frac{1}{2}X^2 + \frac{2}{3}X + 1 \in \mathbb{Q}[X]$$

は原始多項式 $3X^2 + 4X + 6$ と $I(g) = 1/6$ の積である:

$$g = \frac{1}{6}(3X^2 + 4X + 6).$$

例 2.6.10 R を一意分解整域とする. 定数でない $f \in R[X]$ は既約元ならば, 原始多項式である.

補題 2.6.9 (Gauss の補題) R を一意分解整域とし, K をその分数体とする. $f, g \in K[X]$ に対し

$$I(fg) \sim I(f)I(g).$$

特に, 原始多項式の積は原始多項式である.

証明 $f = I(f)f_0$, $g = I(g)g_0$ を内容と原始多項式の積への分解とすると $fg = I(f)I(g)f_0g_0$. 従って, 積 f_0g_0 が原始多項式であることを示せばよい. f_0g_0 が原始多項式でないとすると, すべての係数がある素元 p で割り切れる. $h \in R[X]$ に対しその係数を $R/(p)$ の元と見たものを $\bar{h}$ と表す. (p) は素イデアルであるので $R/(p)$ は整域である. 従って, 例 2.5.3 により $R/(p)[X]$ も整域である.

$$R[X] \longrightarrow R/(p)[X], \quad h \longmapsto \bar{h}$$

を, 例 2.4.3 に於いて定めた, (p) に関する簡約写像とする. すると

$$\overline{f_0g_0} = \bar{f}_0\bar{g}_0 = 0 \in R/(p)[X]$$

従って $\bar{f}_0 = 0$ または $\bar{g}_0 = 0$. すなわち f_0 または g_0 が原始多項式でない. これは不合理. よって f_0g_0 は原始多項式である. □

補題 2.6.10 R を一意分解整域, K をその分数体とする.

(1) $f \in R[X]$ が

$$f = gh, \quad (\deg(g),\ \deg(h) \geq 1)$$

と $K[X]$ において因数分解されるならば,

$$f = g_1h_1, \quad (\deg(g) = \deg(g_1),\ \deg(h) = \deg(h_1))$$

と $R[X]$ で因数分解される.

(2) 定数でない既約多項式 $f \in R[X]$ は $K[X]$ に於いても既約である.

(3) 原始多項式 $f \in R[X]$ が $K[X]$ に於いて既約ならば, $R[X]$ に於いても既約である.

(4) $f, g \in R[X]$ とする. g が原始多項式で, $K[X]$ に於いて $g|f$ ならば, $R[X]$ に於いて $g|f$.

証明 (1) $f = gh$ $(\deg(g), \deg(h) \geq 1)$ と $K[X]$ で因数分解されたとする. g, h を内容と原始多項式の積に表す: $g = I(g)g_0$, $h = I(h)h_0$. このとき, Gauss の補題により, f_0g_0 は原始多項式となり, $I(g)I(h) \sim I(f) \in R$. g_0 を適当に単数倍すれば, $f = I(f)g_0h_0$ としてよい. 従って $g_1 = g_0, h_1 = I(f)h_0 \in R[X]$ とすれば, $f = g_1h_1$. よって, (1) が示された.

上の証明で, g を原始多項式とすれば, $I(g) = 1, g = g_0$ であり, $I(f) = I(h) \in R$ としてよい. 従って, $h_1 = I(f)h_0 = h \in R[X]$. よって (4) を得る. (2) と (3) は, (1) から直ちに得られる. □

補題 2.6.11 R を一意分解整域とする. $R[X]$ の既約元は素元である.

証明 $f \in R[X]$ を既約元とし, $f|gh$ と仮定する.
f が定数の場合. f は R の既約元であり, 補題 2.6.7 から, f は素元であり, $I(f) = f$. $fk = gh$ とすれば, Gauss の補題より, $I(f)I(k) = fI(k) \sim I(g)I(h)$. 従って $f|I(g)$ または $f|I(h)$, すなわち $f|g$ または $f|h$ が成り立つ.
f が定数でない場合. $f|gh$ $(g, h \in R[X])$ とする. 既約元 f は, 補題 2.6.10 (2) により, $K[X]$ の既約元である. $K[X]$ は単項イデアル整域なので, 定理 2.6.8 により, 一意分解整域である. 従って, 補題 2.6.4 により, f は $K[X]$ の素元である. よって $K[X]$ において $f|g$ または $f|h$ が成り立つ. 定数でない既約元 f は原始多項式なので, 補題 2.6.10 (4) により, $R[X]$ に於いて $f|g$ または $f|h$ が成り立つ. よって, f は素元である. □

定理 2.6.12 R が一意分解整域ならば $R[X_1, \cdots, X_n]$ も一意分解整域である.

証明 $n = 1$ のときを示せば, 一般の場合は帰納法から直ちに得られる. $n = 1$ とする. 0 でもなく, 単数でもない任意の元 $f \in R[X]$ が既約元の積に表されることを示す. f が定数ならば, R が一意分解整域なので, f は R の既約元の積に表される. R の既約元は, $R[X]$ の既約元なので, 定数 f は $R[X]$ の既約元の積として表される.
次に f は定数でないとする. $K[X]$ は単項イデアル整域なので, 定理 2.6.8 により, $K[X]$ は一意分解整域である. 従って

$$f = f_1 \cdots f_k, \quad f_i \in K[X]$$

と既約元の積に分解される. f_i に付随する原始多項式を $(f_i)_0$ とすると

$$f = I(f_1) \cdots I(f_k)(f_1)_0 \cdots (f_k)_0.$$

原始多項式 $(f_i)_0$ は $K[X]$ に於いて既約であり, $R[X]$ の既約元である. Gauss の補題により, $I(f) \sim I(f_1) \cdots I(f_k)$. 特に, $I(f_1) \cdots I(f_k) \in R$ となり, これを既約元の積 $p_1 \cdots p_l$ に分解すれば,

$$f = p_1 \cdots p_l (f_1)_0 \cdots (f_k)_0$$

は既約元の積への分解である.
よって, 補題 2.6.7 と補題 2.6.11 を組み合わせて, 定理を得る. □

系 2.6.13 体 k 上の n 変数多項式環 $k[X_1, \cdots, X_n]$ は一意分解整域である.

証明 体は一意分解整域である. 従って, 定理により, $k[X_1, \cdots, X_n]$ は一意分解整域である. □

2.6.4 既約判定法

有理数係数多項式の既約判定法を解説する.
p を素数とし,

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/(p) = \mathbb{F}_p, \quad a \longmapsto [a]$$

を自然な全射とする. 簡約写像

$$\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X], \quad a_n X^n + \cdots a_1 X + a_0 \longmapsto [a_n]X^n + \cdots + [a_1]X + [a_0]$$

による, $f(X) \in \mathbb{Z}[X]$ の像を $\bar{f}(X)$ と表す.

補題 2.6.14 （簡約判定法）p を素数とする．

$$f(X) = a_nX^n + \cdots a_1X + a_0 \in \mathbb{Z}[X], \quad p \nmid a_n$$

に対し，$\bar{f}(X)$ が既約ならば，f は $\mathbb{Q}[X]$ で既約である．

証明 f が $\mathbb{Q}[X]$ で可約とすると，補題 2.6.10 により，$f = gh$ $(\deg(g), \deg(h) > 0)$ と $\mathbb{Z}[X]$ で因数分解される．従って，$\bar{f} = \bar{g}\bar{h}$. $p \nmid a_n$ なので，$\deg(\bar{f}) = n$ であり，$\deg(\bar{g}), \deg(\bar{f}) > 0$. 従って，$\bar{f}$ が可約となる．よって，$f \in \mathbb{Q}[X]$ は既約でなければならない． □

例 2.6.11 $\mathbb{F}_2[X]$ の 4 次以下の既約多項式は以下の通り：

$$X, \quad X+1; \quad X^2+X+1, \quad X^3+X^2+1, \quad X^3+X+1;$$

$$X^4+X^3+1, \quad X^4+X+1, \quad X^4+X^3+X^2+X+1.$$

$p = 2$ として，補題を適用して，

$$X^4 + 2X^3 - 4X^2 + 3X + 7$$

は $\mathbb{Q}[X]$ の既約多項式であることが判る．

例 2.6.12 $\mathbb{F}_3$ 係数 2 次の既約多項式は

$$X^2 + X + 2, \ X^2 + 2X + 1, \ X^2 + 2X + 2$$

の三個である．これらは，$X^5 + X^4 + 2$ を割り切らないので，$X^5 + X^4 + 2 \in \mathbb{F}_3[X]$ は既約多項式である．従って，補題より，

$$X^5 - 5X^4 - 6X - 1 \in \mathbb{Q}[X]$$

は既約多項式である．

定理 2.6.15 （Eisenstein の既約判定法）p を素数とする．整数係数多項式

$$f(X) = a_nX^n + \cdots a_1X + a_0$$

は次を満たすとき，$\mathbb{Q}[X]$ において既約である．

(1) $p \nmid a_n$,

(2) $p|a_{n-1}, \cdots, p|a_0$,

(3) $p^2 \nmid a_0$.

さらに f が原始的ならば，f は $\mathbb{Z}[X]$ において既約である．

証明 $f = gh$ と $\mathbb{Q}[X]$ で因数分解されたとする．このとき，補題 2.6.10 により $g, h \in \mathbb{Z}[X]$ としてよい．条件 (1), (2) より

$$[a_n]X^n = \bar{f} = \bar{g}\bar{h}.$$

従って $\bar{g} = [b_k]X^k, \bar{h} = [c_l]X^l$ と表され，g, h の最高次係数以外の係数は p で割り切れる．また g, h の定数項を b_0, c_0 とすれば，$a_0 = b_0c_0$. 従って $p^2|a_0$. これは (3) に反する．よって f は $\mathbb{Q}[X]$ で既約である．最後の主張は，明らかである． □

例 2.6.13 $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ は既約である.

系 2.6.16 （素数次円分多項式の既約性）p を素数とする. このとき, 円分多項式

$$f(X) = X^{p-1} + \cdots + X + 1 \in \mathbb{Q}[X]$$

は既約である.

証明 $X = Y + 1$ を代入し, Y の多項式 $f(Y+1)$ が既約であることを示せばよい. $f(X) = (X^p - 1)/(X - 1)$ なので, $X = Y + 1$ を代入すると

$$Yf(Y+1) = (Y+1)^p - 1 = Y^p + \binom{p}{1}Y^{p-1} + \binom{p}{2}Y^{p-2} + \cdots + \binom{p}{p-1}Y.$$

従って,

$$f(Y+1) = Y^{p-1} + \binom{p}{1}Y^{p-2} + \cdots + \binom{p}{p-2}Y + \binom{p}{p-1}$$

ここで

$$p|\binom{p}{l},\ l = 1, \cdots, p-1; \quad p^2 \nmid \binom{p}{p-1} = p.$$

従って, Eisenstein の既約判定法により $f(Y+1)$ は既約である. □

2.6.5 Gauss の整数環の素数

この小節では, Gauss の整数環 $\mathbb{Z}[i]$ の素元を決定する.

補題 2.6.17 p を奇素数とし, $\mathbb{F}_p^\times$ の平方数の全体を $(\mathbb{F}_p^\times)^2$ と表す. このとき, 写像

$$\lambda : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}, \quad a \longmapsto a^{(p-1)/2}$$

は群全射であり, $\mathrm{Ker}(\lambda) = (\mathbb{F}_p^\times)^2$.

証明 λ が群射であることは明らか. $\mathbb{F}_p^\times$ は巡回群であり, g をその生成元とする. このとき, $\lambda(g) = -1$ なので, λ は全射である. また, $\lambda(x^2) = \lambda(x)^2 = 1$ も明らか. 逆に,

$$\lambda(g^n) = g^{n(p-1)/2} = 1$$

とすれば, $2|n$ となり, $g^n \in (\mathbb{F}_q^\times)^2$. 以上により, 主張が示された. □

さて, 例 2.6.2 により, $\mathbb{Z}[i]$ は Euclid 整域である. 従って, $\mathbb{Z}[i]$ は, 補題 2.6.1 より, 単項イデアル整域であり, 定理 2.6.8 により, 一意分解整域である.

$\mathbb{Z}[i]$ の整数論を展開する上で, ノルム写像

$$N : \mathbb{C} \longrightarrow \mathbb{R}, \quad N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$$

の果たす役割は大きい.

次は, 定義より, 容易に得られる：

補題 2.6.18 (1) $a+bi \in \mathbb{Z}[i]$ に対し, $N(a+bi)=1 \iff a+bi \in \mathbb{Z}[i]^\times$.

(2) $\mathbb{Z}[i]^\times = \{1, i, -1, -i\} = \langle i \rangle$ は, 位数 4 の巡回群である.

以下, $\mathbb{Z}$ の素数を有理素数といい, $\mathbb{Z}[i]$ の素数は素元といって区別する.
次は, 容易に確かめられる：

補題 2.6.19 $\alpha \in \mathbb{Z}[i]$ が素元ならば, $(\alpha) \cap \mathbb{Z}$ は素イデアルである. 従って,

$$(\alpha) \cap \mathbb{Z} = (p)$$

とすれば, p は素数である. 特に, α は p の約数である.

補題の状況のとき, (α) を (p) の上にある素イデアルということにしよう.

定理 2.6.20 p を有理素数とする.

(1) $\mathbb{Z}$ のイデアル (2) の上にある素イデアルは, $(1+i)$ のみであり, $2\mathbb{Z}[i] = (1+i)^2$.

(2) $p \equiv 1 \pmod 4$ のとき, $p = a^2+b^2$ $(a, b \in \mathbb{N})$ と表される. (p) の上にある素イデアルは, $(a+bi)$, $(a-bi)$ であり, $(p) = (a+bi)(a-bi)$. また, $(a+bi) \neq (a-bi)$.

(3) $p \equiv 3 \pmod 4$ のとき, $p\mathbb{Z}[i]$ は, 素イデアルである.

証明 (1) $1+i = (a+bi)(c+di)$ と二つの整数に因数分解されたとする. $2 = N(1+i) = (a^2+b^2)(c^2+d^2)$ なので, $a+bi, c+di$ のどちらかは, 単数である. よって, $1+i$ は既約元であり, 従って素元である. また, $(1+i)^2 = (2i) = 2\mathbb{Z}[i]$.
(2) 補題 2.6.17 より, $a^2 \equiv -1 \pmod p$ $(\exists a \in \mathbb{Z})$. よって,

$$a^2+1 = (a+i)(a-i) \in p\mathbb{Z}[i] \tag{2.3}$$

であり, $a+i \notin p\mathbb{Z}[i]$, $a-i \notin p\mathbb{Z}[i]$. 即ち, $p\mathbb{Z}[i]$ は素イデアルではない, 即ち p は素元でない. p を素元の積に表す: $p = \alpha\alpha_2 \cdots \alpha_r$ $(r \geq 2)$. すると, $p^2 = N\alpha N\alpha_2 \cdots N\alpha_r$. 従って, $N\alpha \in \{1, p, p^2\}$.
$N(\alpha) = 1$ ならば, α は単数であり, $N(\alpha) = p^2$ ならば, $p = \alpha$ となり不合理. よって, $N(\alpha) = \alpha\bar{\alpha} = p$. $\alpha = a+bi$ とすれば, $p = a^2+b^2$.
次に, $(\alpha) \neq (\overline{\alpha})$ を示そう. 式 (2.3) より,

$$(a+i)(a-i) = a^2+1 \in p\mathbb{Z}[i] \subseteq (\alpha)$$

であり, (α) は素イデアルなので, $a+i \in (\alpha)$ または, $a-i \in (\alpha)$. もし, $(\alpha) = (\overline{\alpha})$ ならば, $a+i, a-i \in (\alpha)$. 従って, $2i \in (\alpha)$. よって, $2, p \in (\alpha)$ となり, $1 \in (\alpha)$. これは不合理.
(3) p が, $\mathbb{Z}[i]$ の素元でないとすると, 単数でない α, β が存在して, $p = \alpha\beta$ と因数分解される. すると, $p^2 = N\alpha N\beta$ であり, $N\alpha = N\beta = p$. $\alpha = a+bi$ とすると $p = a^2+b^2$. a, b が共に偶数ではあり得ないし, 共に奇数でもない. よって, 一方は偶数であり, 他方は奇数である. すると, $p = a^2+b^2 \equiv 1 \pmod 4$ となり, 不合理. □

定理 2.6.21 （Fermat）$p \equiv 1 \pmod 4$ のとき,

$$p = a^2 + b^2 \quad (a, b \in \mathbb{N})$$

と表される. その表し方は, 自明な違いを除いて, 一意的である.

証明 前定理 (2) より, $p = a^2+b^2$ $(a, b \in \mathbb{N})$ と表される. 更に, $p = c^2+d^2 = (c+di)(c-di)$ とすると, $(a+bi)$ は素イデアルなので, $c+di \in (a+bi)$ または, $c-di \in (a+bi)$. $c \pm di = \beta(a+bi)$ $(\exists \beta \in \mathbb{Z}[i])$ とすると, ノルムを比べて, β は単数. 従って, 表し方は一意的である. □

2.7 対称式と交代式

2.7.1 対称式と基本対称式

可換環 R 上の n 変数多項式環 $R[X_1, \cdots, X_n]$ を考える. n 文字の置換 σ と多項式 $f \in R[X_1, \cdots, X_n]$ に対し

$$(\sigma f)(X_1, \cdots, X_n) = f(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$$

と定める. 即ち, 多項式 $f(X_1, \cdots, X_n)$ に於いて, 変数 X_i を $X_{\sigma(i)}$ に置き換えたものが, σf である. このとき, 写像

$$R[X_1, \cdots, X_n] \longrightarrow R[X_1, \cdots, X_n], \quad f \longmapsto \sigma f$$

は環同型射であり, 次を満たす:

(1) $(\sigma\tau)f = \sigma(\tau f)$ $(\forall \sigma, \tau \in S_n,\ \forall f)$,

(2) $1f = f$ $(1 \in S_n)$.

任意の置換 $\sigma \in S_n$ に対し,

$$\sigma f = f$$

を満たす多項式 $f(X_1, \cdots, X_n)$ を, **対称多項式**という.

例 2.7.1 $n+1$ 変数多項式

$$\begin{aligned} F(T, X_1, \cdots, X_n) &= (T - X_1)(T - X_2) \cdots (T - X_n) \\ &= T^n - s_1 T^{n-1} + \cdots + (-1)^n s_n \end{aligned}$$

を考える. このとき n 変数多項式

$$\begin{aligned} s_1 &= X_1 + X_2 + \cdots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\ &\cdots \\ s_n &= X_1X_2 \cdots X_n \end{aligned}$$

は, 対称多項式であり, **基本対称式** と呼ばれる.

$T_1, \cdots, T_n$ を変数とする単項式

$$T_1^{r_1} T_2^{r_2} \cdots T_n^{r_n} \in R[T_1, \cdots, T_n] \tag{2.4}$$

に対し

$$r_1 + 2r_2 + \cdots + nr_n$$

を, この単項式の**重さ** という. また, 多項式

$$g(T_1, \cdots, T_n) \in R[T_1, \cdots, T_n]$$

に現れる単項式の重さの最大値を, 多項式 g の **重さ** といい, $\mathrm{weight}(g)$ と表す.

例 2.7.2 $g \in R[T_1, \cdots, T_n]$ の重さを w とするとき, $g(s_1, s_2, \cdots, s_n)$ の $X_1, \cdots, X_n$ に関する次数は w である.

定理 2.7.1 任意の対称多項式は, 基本対称式の多項式として一意的に表される. すなわち, 対称多項式 f に対し,

$$f(X_1, \cdots, X_n) = g(s_1, \cdots, s_n)$$

を満たす多項式 g が一意的に存在する.

証明 環射

$$\phi : R[T_1, \cdots, T_n] \longrightarrow R[X_1, \cdots, X_n], \quad T_i \longmapsto s_i$$

を考える.

任意の対称多項式が, 基本対称式の多項式として表されることは, $\mathrm{Im}(\phi)$ が対称多項式のなす $R[X_1, \cdots, X_n]$ の部分環に一致することである. このことを, 変数の個数 n に関する帰納法で示す. $n = 1$ の場合は明らかである. $n - 1$ の場合に定理が成り立つとする. n の場合, 次数 d に関する帰納法で示す. $d = 0$ のときは明らか. $d > 0$ とする. 次数 d の対称多項式 $f \in R[X_1, \cdots, X_n]$ に対し

$$f^0(X_1, \cdots, X_{n-1}) = f(X_1, \cdots, X_{n-1}, 0)$$

とする. すると帰納法の仮定により, 多項式 $g \in R[T_1, \cdots, T_{n-1}]$ が存在して

$$f^0(X_1, \cdots, X_{n-1}) = g(s_1^0, \cdots, s_{n-1}^0)$$

と表される. ただし

$$s_1^0 = X_1 + \cdots + X_{n-1}, \ \cdots, \ s_{n-1}^0 = X_1 \cdots X_{n-1}$$

は, $n - 1$ 変数の基本対称式である. 次数に関して

$$\deg(f) \geq \deg(f^0) = \mathrm{weght}(g)$$

が成り立つことに注意する. 対称多項式

$$f_1(X_1, \cdots, X_n) := f(X_1, \cdots, X_n) - g(s_1, \cdots, s_{n-1})$$

は, $\deg(f_1) \leq d$ を満たす. $f_1(X_1, \cdots, X_{n-1}, 0) = 0$ なので, 剰余の定理より, $X_n | f_1$. f_1 の対称性により, すべての i に対し $X_i | f_1$. 従って $s_n | f_1$ となり, 対称多項式 h が存在して

$$f(X_1, \cdots, X_n) = g(s_1, \cdots, s_{n-1}) + s_n h(X_1, \cdots, X_n)$$

と表される. h の次数は d より小さいので, h は基本対称式の多項式である. 従って f も基本対称式の多項式である. よって n の場合が示された.

次に一意性を示そう. 一意性は, $\mathrm{Ker}(\phi) = \{0\}$ のことである. このことを, n に関する帰納法で示す. $n = 1$ の場合は明らかで $n - 1$ の場合, 主張は正しいとする. n の場合, 次数に関する帰納法で示す. $g \in \mathrm{Ker}(\phi)$ に対し, $g(s_1, \cdots, s_n) = 0$ なので, 特に, $g(s_1^0, \cdots, s_{n-1}^0, 0) = 0$. 但し, $s_i^0 = s_i(X_1, \cdots, X_{n-1}, 0)$ と定める. すると, $n - 1$ の場合なので, $g(T_1, \cdots, T_{n-1}, 0) = 0$. よって, 剰余の定理により, $g(T) = T_n h(T)$ と表され,

$$g(s_1, \cdots, s_n) = s_n h(s_1, \cdots, s_n) = 0.$$

$s_n = X_1 \cdots X_n$ は $R[X_1, \cdots, X_n]$ に於いて, 零因子ではないので $h(s_1, \cdots, s_n) = 0$. h の次数は g の次数より小さいので, $h(T_1, \cdots, T_n) = 0$ となり, $g(T_1, \cdots, T_n) = 0$. 以上により, $\mathrm{Ker}(\phi) = \{0\}$ となり, 一意性が示された. □

例 2.7.3 整係数対称式 $f(X_1, X_2, X_3) = \{(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)\}^2$ に対し

$$f(X_1, X_2, 0) = \{(X_1 - X_2)X_1X_2\}^2 = ((X_1 + X_2)^2 - 4X_1X_2)(X_1X_2)^2 = ((s_1^0)^2 - 4s_2^0)(s_2^0)^2.$$

$$f(X_1, X_2, X_3) = ((s_1)^2 - 4s_2)(s_2)^2 + s_3 h(s_1, s_2, s_3) \quad \exists h(T_1, T_2, T_3) \in \mathbb{Z}[T_1, T_2, T_3] \tag{2.5}$$

と表される. 但し, h は対称式である. $h(s_1, s_2, s_3)$ の X_1, X_2, X_3 に関する次数は 3 である. 従って

$$h = as_1^3 + bs_1s_2 + cs_3, \quad a, b, c \in \mathbb{Z}$$

と表される. 式 (2.5) の (X_1, X_2, X_3) に $(1, 1, 1), (1, 1, -1), (-1, 1, 2)$ を代入し

$$\begin{aligned} 0 &= -27 + 27a + 9b + c \\ 0 &= 5 - a + b + c \\ 36 &= 8 - 2(8a - 2b - 2c). \end{aligned}$$

よって, $(a, b, c) = (-4, 18, -27)$ となり

$$f = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2.$$

例 2.7.4

$$F(X_1, X_2, X_3, X_4) = (X_1 + X_2 - (X_3 + X_4))(X_1 + X_3 - (X_2 + X_4))(X_1 + X_4 - (X_2 + X_3))$$

は, 三次の同次式なので,

$$F(X_1, X_2, X_3, X_4) = As_1^3 + Bs_1s_2 + Cs_3$$

と, 表される. $X_2 = X_3 = X_4 = 0$ を代入し, $A = 1$. $X_3 = X_4 = 0$ を代入し, $B = -2$. $X_1 = X_2 = X_3 = 1, X_4 = 0$ を代入し, $C = -10$. 従って,

$$F(X_1, X_2, X_3, X_4) = s_1^3 - 4s_1s_2 + 8s_3.$$

2.7.2 交代式と差積

定義 2.7.2 任意の置換 $\sigma \in S_n$ に対し,

$$\sigma f = \mathrm{sign}(\sigma) f$$

を満たす多項式 $f \in R[X_1, \cdots, X_n]$ を, **交代多項式**, 或いは, 単に, **交代式** という.

例 2.7.5 多項式

$$\Delta = \prod_{1 \le i < \le j} (X_i - X_j)$$

を **差積** という. Δ は整係数交代式である.

定理 2.7.3 $\mathbb{Z}[X_1, \cdots, X_n]$ に含まれる任意の交代多項式は, 差積と対称多項式の積として表される.

証明 $f(X_1, \cdots, X_n)$ を交代式とする.

$$f(X_1, \cdots, X_i, \cdots, X_j, \cdots, X_n) = -f(X_1, \cdots, X_j, \cdots, X_i, \cdots, X_n)$$

なので, $X_i - X_j | f$. $(i, j) \neq (k, l)$ ならば, $X_i - X_j$ と $X_k - X_l$ は, $\mathbb{Z}[X_1, \cdots, X_n]$ の異なる素元なので, $\Delta | f$. $f = \Delta g$ と表せば, g は明らかに対称式である. □

例 2.7.6 k を体とし, k 係数 n 次代数方程式

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n = 0$$

の n 個の根を $\alpha_1, \cdots, \alpha_n$ とする. このとき

$$D(f) = a_0^{2(n-1)} \left(\prod_{1 \le i \le j \le n} (\alpha_i - \alpha_j) \right)^2$$

を方程式 f （又は多項式 f ）の **判別式** という.

二次方程式 $aX^2 + bX + c = 0$ の判別式は $b^2 - 4ac$ であり, 三次方程式 $a_0 X^3 + a_1 X^2 + a_2 X + a_3 = 0$ の判別式は, 例 2.7.3 により,

$$a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_0 a_2^3 + 18 a_0 a_1 a_2 a_3 - 27 a_0^2 a_3^2.$$

特に, 三次方程式 $X^3 + pX + q = 0$ の判別式は $-4p^3 - 27q^2$ に等しい.

第3章　体

体の最も基本的な例は, 有理数体 $\mathbb{Q}$, 素数個の元からなる有限体 $\mathbb{F}_p$ と x を変数とする体 k 上の有理関数体 $k(x)$ である. これらの体の元を係数とする代数方程式の解を考察の対象とすることから, 定まった体を含む体, 即ち拡大体の研究が促された. そこで, 体の拡大から論じよう.

3.1　体の拡大

3.1.1　基本的事項

体 k が体 K の部分体のとき, K を k の **拡大体** という. このとき K/k と表し, **体の拡大** という. K と k との中間にある体を拡大 K/k の**中間体** という.

例 3.1.1 $\mathbb{C}/\mathbb{Q}$ は体の拡大である. $\mathbb{C}/\mathbb{Q}$ の中間体を **数体** という.

k を体とすると, 有理整数環 $\mathbb{Z}$ から k への環射 $\phi : \mathbb{Z} \longrightarrow k$ が, 常に唯一つ存在する：

$$\phi(n) = \begin{cases} \overbrace{1 + \cdots + 1}^{n} & (n > 0) \\ 0 & n = 0 \\ \overbrace{(-1) + \cdots + (-1)}^{-n} & (n < 0) \end{cases}$$

$\mathbb{Z}$ は単項イデアル整域なので, $\mathrm{Ker}(\phi) = (d)$ となる非負整数 d が存在する. このとき, 環射の分解定理（定理 **??**により, 環単射

$$\phi_* : \mathbb{Z}/(d) \longrightarrow k$$

が存在し, $\mathbb{Z}/(d) \simeq \phi_*(\mathbb{Z}/(d))$ である. $\phi_*(\mathbb{Z}/(d))$ は, 体 k の部分環なので, 整域である. 従って, d は 0 であるか素数である. d を体 k の **標数** といい, $\mathrm{char}(k)$ と表す.

$\mathrm{char}(k) = 0$ のとき, $\phi : \mathbb{Z} \longrightarrow k$ は環単射であり, ϕ は $\mathbb{Z}$ の分数体 $\mathbb{Q}$ から k への環単射 $\tilde{\phi}$ に延長される：

$$\tilde{\phi}(a/b) = \phi(a)/\phi(b) \quad (\forall a/b \in \mathbb{Q}).$$

よって, k は有理数体と同型な体 $\tilde{\phi}(\mathbb{Q})$ を含む.

$\mathrm{char}(k) = p$ が素数のとき, $\mathbb{Z}/(p) = \mathbb{F}_p \simeq \phi_*(\mathbb{F}_p)$ であり, k は有限体 $\mathbb{F}_p$ と同型な体 $\phi_*(\mathbb{F}_p)$ を含む.

K/k を体の拡大とし, S を K の部分集合とする. k と S を含む K の部分体の全体を $\{K_i\}_{i \in I}$ とするとき,

$$k(S) = \cap_{i \in I} K_i$$

は, k と S を含む K 最小の部分体である.

問 3.1.1 $k(S)$ が k と S を含む K 最小の部分体であることを確認せよ.

$k(S)$ を k 上 S で **生成された体**, または k に S を **添加した体** という. 特に $S = \{\alpha_1, \cdots, \alpha_n\}$ のとき

$$k(S) = k(\alpha_1, \cdots, \alpha_n)$$

と表す. k に有限個の元を添加して得られる体を k 上 **有限生成体** という. $S = \{\alpha\}$ のとき, $k(\alpha)/k$ を **単純拡大** といい, α を拡大 $k(\alpha)/k$ の **原始元** という.

例 3.1.2 $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ であり, $\sqrt{-1}$ は, 拡大 $\mathbb{C}/\mathbb{R}$ の原始元である.

問 3.1.2

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

を確かめよ.

問 3.1.3 K/k を体の拡大とし,

$$\{\alpha_1, \cdots, \alpha_n\} \subset K$$

に対し,

$$k(\alpha_1, \cdots, \alpha_n) = \left\{ \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} \;\middle|\; f, g \in k[X_1, \cdots, X_n], g(\alpha_1, \cdots, \alpha_n) \neq 0 \right\}$$

を示せ.

例 3.1.3 E, F を体 L の部分体とする. このとき $E(F) = F(E)$ は E と F を含む L の最小の部分体で, EF と表され, E と F との **合成体** と呼ばれる.

問 3.1.4 体 E, F の合成体 EF の各元は

$$\frac{a_1b_1 + \cdots + a_nb_n}{c_1d_1 + \cdots + c_md_m}, \quad a_i, c_j \in E, \quad b_i, d_j \in F \quad (i = 1, \cdots, n; j = 1, \cdots, m)$$

と表されることを示せ.

3.1.2 有限次拡大と拡大次数

K/k を体の拡大とする. このとき, K の乗法を制限して得られる写像

$$\cdot : k \times K \longrightarrow K$$

をスカラー倍として, $(K; +, \cdot)$ は k 上のベクトル空間である.

問 3.1.5 $(K; +, \cdot)$ は体 k 上のベクトル空間であることを確かめよ.

k 上のベクトル空間 K の次元 $\dim_k(K)$ を拡大 K/k の **拡大次数** といい, $[K:k]$ と表す. $[K:k]=n$ のとき, K/k を n **次拡大** という. 一般に $[K:k]$ が有限, 或いは, 無限のとき, K/k を **有限次拡大**, 或いは, **無限次拡大** という.

例 3.1.4

$$[\mathbb{C}:\mathbb{R}]=2, \quad [\mathbb{R},\mathbb{Q}]=\infty.$$

例 3.1.5 n を平方数でない整数とする. このとき $\mathbb{Q}(\sqrt{n})$ は $\mathbb{Q}$ 上 2 次拡大である. 実際, $1,\sqrt{n}$ が $\mathbb{Q}$ 上のベクトル空間 $\mathbb{Q}(\sqrt{n})$ の基底である. n が正のとき, $\mathbb{Q}(\sqrt{n})$ は実数体 $\mathbb{R}$ の部分体であり, **実二次体** と呼ばれる. 一方 n が負のとき, $\mathbb{Q}(\sqrt{n})$ は実数体に含まれず, **虚二次体** と呼ばれる.

補題 3.1.6 $k\subset F\subset E$ を体の拡大とするとき,

$$[E:k]=[E:F][F:k]$$

が成り立つ.

特に, E/F, F/k が有限次拡大ならば, E/k も有限次拡大である.

証明 $\{x_1,\cdots,x_m\}$ を F の k 上の基底とし, $\{y_1,\cdots,y_n\}$ を E の F 上の基底とする. このとき $\{x_iy_j\}_{1\le i\le m,1\le j\le n}$ が E の k 上の基底となる. □

例 3.1.6 $\omega=\frac{-1+\sqrt{-3}}{2}\in\mathbb{C}$ と $\sqrt{2}$ を有理数体に添加した体を $K=\mathbb{Q}(\omega,\sqrt{2})$ とする. このとき, $K=(\mathbb{Q}(\sqrt{2}))(\omega)$ であり,

$$[K:\mathbb{Q}]=[K:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\cdot 2=4.$$

問 3.1.7 K/k が素数次拡大ならば, K と k の真の中間体は存在しないことを確かめよ.

3.1.3 代数拡大

体 k の元を係数とする一変数 n 次多項式 $f(X)$ に対し, 方程式 $f(X)=0$ を k 係数 n 次 **代数方程式** という. $f(\alpha)=0$ を満たす $\alpha\in k$ を $f(X)$ の **根** という.

K/k を体の拡大とし, $\alpha\in K$ とする. α を根に持つ 1 次以上の k 係数多項式 $g(X)\in k[X]$ が存在するとき, α は k 上 **代数的** であるという. そのような多項式のうち次数が最小のものを α の k 上の **最小多項式** という. 最小多項式は, 零でない定数倍を除いて一意的に定まる. 以下特に断らない限り, 最小多項式の最高次係数は 1 とする.

α を根に持つ k 係数多項式が存在しないとき, α は k 上 **超越的** であるという.

問 3.1.8 最小多項式は, 定数倍を除いて一意的に定まることを確かめよ.

例 3.1.7 X^2+X+1 は $\omega=\frac{-1+\sqrt{-3}}{2}$ の $\mathbb{Q}$ 上の最小多項式である. 虚数単位 $\sqrt{-1}$ の $\mathbb{R}$ 上の最小多項式は X^2+1 である.

例 3.1.8 $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式は X^4-2 である.

問 3.1.9 $\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.

例 3.1.9 有理数体 $\mathbb{Q}$ 上代数的な複素数を **代数的数** といい, $\mathbb{Q}$ 上超越的な複素数を **超越数** という. $\sqrt{2}, \sqrt{-1}$ は代数的数である. 円周率 π, 自然対数の底 e は超越数であるが, その証明は容易ではない.

定理 3.1.10 K/k を体の拡大とし, $\alpha \in K$ とする. このとき次が成り立つ.

(1) α が k 上超越的ならば, $k(\alpha)$ は k 上の一変数有理関数体 $k(X)$ に同型である.

(2) α が k 上代数的ならば, $p(X)$ をその最小多項式とするとき, 体同型射

$$\phi : k[X]/(p(X)) \longrightarrow k(\alpha) \text{ s.t. } \phi([X]) = \alpha,\ \phi|k = \mathrm{id}_k$$

が存在する. また $n = \deg(p(X))$ とするとき, $[k(\alpha) : k] = n$, であり, $(1, \alpha, \cdots, \alpha^{n-1})$ は $k(\alpha)$ の k 上の基底である. 更に, $k(\alpha) = k[\alpha]$ が成り立つ.

証明 (1) α が k 上超越的なので, 環射

$$\phi : k[X] \longrightarrow k(\alpha), \quad X \longmapsto \alpha$$

は, 単射である. 分数体の普遍性（定理 2.5.12）, 即ち, $\tilde{\phi}(f/g) = \phi(f)/\phi(g)$ と定めることにより, 体同型射 $\tilde{\phi} : k(X) \longrightarrow k(\alpha)$ を得る.
(2) α を k 上代数的とする. 一変数多項式環 $k[X]$ から K への環射

$$\phi : k[X] \longrightarrow K, \quad g(X) \longmapsto g(\alpha)$$

を考える. $k[X]$ は単項イデアル整域なので, $\mathrm{Ker}(\phi) = (p(X))$ となる多項式 $p(X)$ が存在する. このとき, $p(X)$ は α の最小多項式である. 環の同型定理 **??** により

$$k[X]/(p(X)) \simeq k[\alpha] = \mathrm{Im}(\phi).$$

体 K の部分環 $k[\alpha]$ は整域なので, 補題 2.5.8 により, $(p(X))$ は素イデアルである. $k[X]$ は単項イデアル整域なので, 補題 2.6.6 により, 0 と異なる素イデアル $(p(X))$ は極大イデアルである. 従って, 補題 2.5.5 により, $k[X]/(p(X))$ は体である. よって $k[\alpha]$ も体であり, $\alpha \in k[\alpha] \subset k(\alpha)$. 従って, $k(\alpha)$ を k と α を含む最小の体として定義したので, $k[\alpha] = k(\alpha)$ を得る.
$p(X)$ は α の最小多項式なので, $n = \deg(p(X))$ とすれば, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ は k 上一次独立であり, かつ, $k[\alpha] = k(\alpha)$ を生成する. 従って, $(1, \alpha, \cdots, \alpha^{n-1})$ は $k(\alpha)$ の k 上の基底である. □

例 3.1.10 $\sqrt{2}$ は $\mathbb{Q}$ 上代数的なので, 定理より, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. 一方, 有理化により, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ を得る. 従って, 定理は有理化の一般化を与えていると見なすことができる.

定義 3.1.11 体の拡大 K/k に於て K の全ての元が k 上代数的の時, 拡大 K/k を **代数拡大** という. 代数拡大でない拡大を **超越拡大** という.

補題 3.1.12 K/k が有限次拡大ならば, K/k は代数拡大である.

証明 $n=[K:k]$ とする. 任意の $\alpha\in K$ に対し, $\{1,\alpha,\cdots,\alpha^n\}$ は, k 上一次独立ではあり得ない. 従って, $a_0+a_1\alpha+\cdots+a_n\alpha^n=0$ となる $0\neq(a_0,\cdots,a_n)\in k^n$ が存在する. 従って α は k 上代数的である. □

定理 3.1.13 *$K=k(\alpha_1,\cdots,\alpha_n)$ において, 全ての α_i が k 上代数的ならば, K/k は有限次代数拡大であり*

$$K=k(\alpha_1,\cdots,\alpha_n)=k[\alpha_1,\cdots,\alpha_n].$$

証明 n に関する帰納法で示す. $K_i=k(\alpha_1,\cdots,\alpha_i)$ $(i=1,\cdots,n)$ と置く. $n=1$ のときは, 定理 3.1.10 と補題 3.1.12 を組み合わせればよい.

$n=i$ のとき, 定理は正しいとし, $n=i+1$ とする. α_{i+1} は k 上代数的なので, $K_i=k(\alpha_1,\cdots,\alpha_i)=k[\alpha_1,\cdots,\alpha_i]$ 上代数的である. 再び, 定理 3.1.10 により,

$$k(\alpha_1,\cdots,\alpha_{i+1})=K_i(\alpha_{i+1})=K_i[\alpha_{i+1}]=k[\alpha_1,\cdots,\alpha_{i+1}].$$

K_{i+1}/K_i は, 補題 3.1.12 により有限次拡大である. 従って, 補題 3.1.6 により, K_{i+1}/k は有限次拡大であり, 補題 3.1.12 により, 代数拡大となる. □

系 3.1.14 *K/k を体の拡大とし, k 上代数的な K の元全体を L とする. このとき L は K/k の中間体であり, L/k は代数拡大である. L を K における k の* **代数閉包** *という.*

証明 L が K/k の中間体であることを示せば, L の定義により L/k は代数拡大である. L は明らかに k を含む. 従って L が K の部分体であることを示せばよい. L の任意の元 α,β に対し, 定理により $k(\alpha,\beta)/k$ は代数拡大であり, $k(\alpha,\beta)\subset L$. 特に $\alpha+\beta,\alpha\beta\in L$ であり, $\alpha\neq0$ ならば, $\alpha^{-1}\in L$. よって L が K の部分体であることがわかった. □

例 3.1.11 代数的数の全体 $\bar{\mathbb{Q}}$ は, 有理数体 $\mathbb{Q}$ の複素数体 $\mathbb{C}$ に於ける代数閉包である.

問 3.1.15 次を証明せよ.

(1) F を体の拡大 L/k の中間体とする. このとき

$$L/k:\text{代数拡大}\quad\Longleftrightarrow\quad L/F,F/k:\text{代数拡大}.$$

(2) E,F を体の拡大 L/k の中間体とする.

$$E/k:\text{代数拡大}\quad\Longrightarrow\quad EF/F:\text{代数拡大}.$$

(3) E,F を体の拡大 L/k の中間体とする.

$$E/k,F/k:\text{代数拡大}\quad\Longrightarrow\quad EF/k:\text{代数拡大}.$$

問 3.1.16 次を証明せよ.

(1) F を体の拡大 L/k の中間体とする. このとき

$$E/k:\text{有限次拡大}\quad\Longleftrightarrow\quad E/F,F/k:\text{有限次拡大}.$$

(2) E, F を体の拡大 L/k の中間体とする.

$$E/k : \text{有限次拡大} \quad \Longrightarrow \quad EF/F : \text{有限次拡大}.$$

(3) E, F を体の拡大 L/k の中間体とする.

$$E/k, F/k : \text{有限次拡大} \quad \Longrightarrow \quad EF/k : \text{有限次拡大}.$$

3.1.4 代数閉体と代数閉包

Ω を体とする. 定数でない Ω 係数の任意の多項式が Ω に於て解を持つとき, Ω を **代数閉体** という.

C.F. Gauss により証明された次の定理は基本的である. ガロア理論を利用した代数的な証明を 4.1.3 で与える.

定理 3.1.17 （代数学の基本定理）複素数体 $\mathbb{C}$ は代数閉体である.

ここでは, 複素関数論で学ぶ Liouville の定理とコンパクト集合の性質を利用した証明を紹介する:

定理 3.1.18 （Liouville の定理）全複素平面上有界な正則関数は定数に限る.

定理 3.1.19 $C \subset \mathbb{C}$ をコンパクト集合とし, $\phi : \mathbb{C} \longrightarrow \mathbb{R}$ を連続写像とする. このとき, $\phi(C)$ は $\mathbb{R}$ のコンパクト集合である.

定理 3.1.17 の証明 $f(z) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ を複素係数 $n\ (\geq 1)$ 次多項式とする. $f(X) = 0$ が複素数根を持たなければ, $g(z) = 1/f(z)$ は定数でない全複素平面上の正則関数である.

$$|z^n + a_{n-1}z^{n-1} + \cdots + a_0| \geq |z|^n - |a_{n-1}z^{n-1} + \cdots + a_0|$$

であり, $|z| = r$ を十分大きくとれば,

$$|a_{n-1}z^{n-1} + \cdots + a_0| < \frac{1}{2}|z|^n.$$

従って, $\{|z| > r\}$ に於いて,

$$|f(z)| > |z|^n - |a_{n-1}z^{n-1} + \cdots + a_0| > \frac{1}{2}|z|^n.$$

即ち,

$$|g(z)| = \frac{1}{|f(z)|} < \frac{2}{r^n}$$

となり, $g(z)$ 有界である. また, $\{|z| \leq r\}$ はコンパクトなので, $1/f(z)$ は, そこでは有界である. 従って, $1/f(z)$ は全平面で有界となり, Liouville の定理により定数でなければならない. これは不合理である. よって, $f(X) = 0$ は複素数根を持つ. □

補題 3.1.20 体 Ω について次は同値である.

(1) Ω は代数閉体である.

(2) Ω の代数拡大は Ω に限る.

(3) $\Omega[X]$ の既約多項式は一次式である.

(4) $\Omega[X]$ の一次以上の多項式は $\Omega[X]$ において一次式の積に因数分解される.

証明 (1) $\Longrightarrow$ (2) L/Ω を代数拡大とする. L の任意元 α をとり, その Ω 上の最小多項式を $f(X)$ とする. 仮定により $f(\beta)=0$ となる $\beta\in\Omega$ が存在する. $\alpha=\beta$ ならば $\alpha\in\Omega$ である. さもなければ

$$g(X)=f(X)/(X-\beta)\in\Omega[X]$$

であり, $g(\alpha)=0$. これは $f(X)$ が最小多項式である事に反する.
(2) $\Longrightarrow$ (3) 既約多項式 $f(X)\in\Omega[X]$ が生成するイデアル $(f(X))\subset\Omega[X]$ は極大イデアルである. 環単射

$$\Omega\longrightarrow\Omega[X]/(f(X)),\quad \omega\longmapsto[\omega]$$

により, $\Omega[X]/(f(X))$ を Ω の拡大体と見なす. このとき, $\Omega[X]/(f(X))$ は Ω の代数拡大で, その拡大次数は $\deg(f)$ に等しい. 仮定より $\Omega[X]/(f(X))=\Omega$ なので, $\deg(f)=1$ でなければならない.
(3) $\Longrightarrow$ (4), (4) $\Longrightarrow$ (1) は明らか. □

定義 3.1.21 L/k が代数拡大で, L が代数閉体のとき, L を k の **代数閉包** という.

例 3.1.12 代数的数全体のなす体 $\bar{\mathbb{Q}}$ は $\mathbb{Q}$ の代数閉包である. $\bar{\mathbb{Q}}/\mathbb{Q}$ の任意の中間体を **代数体** という. 任意の代数体 K に対し, $\bar{\mathbb{Q}}$ は, K の代数閉包である.

問 3.1.22 k を体とし, Ω を k を含む代数閉体とする. k の Ω に於ける代数閉包を $\bar{k}$ と表す. このとき, $\bar{k}$ は代数閉体であること, 即ち, $\bar{k}$ は k の代数閉包であることを確かめよ.

問 3.1.23 K/k を代数拡大とし, L を K の代数閉包とするとき, L は k の代数閉包であることを確かめよ.

与えられた体に対し, その代数閉包の存在を証明する為に, まず, 一つの多項式に対し, その根を含む体の存在を示す.

補題 3.1.24 k を体とし, $f(X)\in k[X]$ を次数 1 以上の多項式とする. このとき, 有限次拡大 K/k が存在して, $f(X)=0$ は K に於て根を持つ.

証明 $f(X)$ を既約多項式の積に因数分解し $g(X)$ をその一つの因数とする. $(g(X))$ は $k[X]$ の極大イデアルなので, $k[X]/(g(X))$ は体である. 自然な環全射 $\sigma:k[X]\longrightarrow k[X]/(g(X))$ を k に制限した写像 $\sigma|_k:k\longrightarrow k[X]/(g(X))$ は環単射である. これにより k とその像を同一視する. この同一視により, $k[X]/(g(X))$ は k の有限次拡大体となる. $\sigma(X)=\zeta$ とすると

$$0=\sigma(g(X))=g(\sigma(X))=g(\zeta).$$

従って $0=\sigma(f(X))=f(\zeta)$ であり, $k[X]/(g(X))$ が求めるものである. □

帰納法を用いて, 直ちに次を得る.

系 3.1.25 k を体とし, $f(X) \in k[X]$ を次数 1 以上の多項式とする. このとき, 有限次拡大 K/k が存在して, $f(X)$ は $K[X]$ で一次式の積に因数分解する.

定理 3.1.26 （代数閉包の存在定理）任意の体 k に対し, k の代数閉包 L が存在する.

証明 $k[X]$ の既約多項式で, 最高次係数が 1 であるものの全体を

$$\{f_\lambda(X)|\lambda \in \Lambda\}$$

とし, $\deg(f_\lambda) = n_\lambda$ とする. 各 λ に対し, 方程式 $f_\lambda(X) = 0$ の n_λ 個の根を構成しよう. その為に変数 $X_1^{(\lambda)}, \cdots, X_{n_\lambda}^{(\lambda)}$ を導入し

$$g_\lambda(X, X_1^{(\lambda)}, \cdots, X_{n_\lambda}^{(\lambda)}) = f_\lambda(X) - \prod_{i=1}^{n_\lambda}(X - X_i^{(\lambda)})$$

と置く. これを

$$g_\lambda(X, X_1^{(\lambda)}, \cdots, X_{n_\lambda}^{(\lambda)}) = \sum_{j=0}^{n_\lambda - 1} A_j^{(\lambda)} X^j, \quad A_j^{(\lambda)} \in k[X_1^{(\lambda)}, \cdots, X_{n_\lambda}^{(\lambda)}]$$

と書換える. $X_i^{(\lambda)}$ が $f_\lambda(X) = 0$ の根となるには, これら $A_j^{(\lambda)}$ は, 全て, 0 とならなくてはならない.

そのような世界を構成しよう. まず, 無限個の変数の多項式環

$$R = k[X_i^{(\lambda)}|\lambda \in \Lambda,\ i = 1, \cdots, n_\lambda]$$

を考え, 全ての $A_j^{(\lambda)}$ に依り生成される R のイデアルを I とする. すると, $I \neq R$. 何故ならば $1 \in I$ とすると

$$1 = \sum A_j^{(\lambda)} B_j^{(\lambda)}, \quad B_j^{(\lambda)} \in R \tag{3.1}$$

と表される. この和は勿論有限個の和である. この和に現れる全ての λ に対し, 上述の系により, 有限次拡大体 E/k が存在し, E において $f_\lambda(X)$ が一次式の積に分解される. そこで

$$f_\lambda(X) = \prod_{i=1}^{n_\lambda}(X - \alpha_i^{(\lambda)}), \quad \alpha_i^{(\lambda)} \in E$$

とすると,

$$g_\lambda(X, \alpha_1^{(\lambda)}, \ldots, \alpha_{n_\lambda}^{(\lambda)}) = 0.$$

これは

$$A_j^{(\lambda)}(\alpha_1^{(\lambda)}, \ldots, \alpha_{n_\lambda}^{(\lambda)}) = 0 \quad (j = 0, \cdots, n_\lambda - 1)$$

を意味する. これを, 式 (3.1) に代入すると, $1 = 0$ となり矛盾である. 従って $I \neq R$ がわかった.

系 2.5.3 により I を含む極大イデアル M が存在する. 従って $L = R/M$ とすれば, これは体である. 自然な環全射

$$\pi : R \longrightarrow L$$

に対し, $\pi(X_i^{(\lambda)}) = \xi_i^{(\lambda)}$ とする.

$$f_\lambda(X) \equiv \prod (X - X_i^{(\lambda)}) \pmod{M}$$

なので, $L[X]$ に於て

$$f_\lambda(X) = \prod (X - \xi_i^{(\lambda)})$$

と一次式の積に分解される.

$$L = k[\xi_i^{(\lambda)} | \lambda \in \Lambda,\ i = 1, \ldots, n_\lambda]$$

であり, 各 $\xi_i^{(\lambda)}$ は k 上代数的である. 従って, 系-定義 3.1.14 より, L/k は代数拡大である.

最後に L が代数閉体である事を示そう. α が L 上代数的とすると, 補題 3.1.15 により k 上代数的である. $f(X)$ を α の k 上の最小多項式とする. $f(X)$ は k 上の既約多項式なので, $f(X) = f_\lambda(X)$ $(\exists \lambda \in \Lambda)$ となる. 従って L の作り方から

$$f(X) = f_\lambda(X) = (X - \alpha_1) \cdots (X - \alpha_d), \quad d = \deg(f),\ \alpha_i \in L$$

と分解される. 従って α はある α_i と一致し, α は L に含まれる. よって, 補題 3.1.20 により, L は代数閉体である. □

3.1.5 超越拡大

K/k を体の拡大とし, $\{\alpha_1, \cdots, \alpha_n\}$ を K の部分集合とする. n 変数多項式環から K への環射

$$k[X_1, \cdots, X_n] \longrightarrow K, \quad X_i \longmapsto \alpha_i \quad (1 \leq i \leq n)$$

が単射のとき, 即ち, $f(\alpha_1, \cdots, \alpha_n) = 0$ となる非自明な多項式 $f(X_1, \cdots, X_n)$ が存在しないとき, $\{\alpha_1, \cdots, \alpha_n\}$ は, k 上 **代数的に独立である** という.

K の部分集合 S の任意の有限部分集合が代数的独立のとき, S は k 上 **代数的に独立である** という.

例 3.1.13 K/k を体の拡大とする. $\alpha \in K$ に対し, 次は同値である:

(1) α は k 上超越的である,

(2) $\{\alpha\}$ は, k 上代数的に独立である.

例 3.1.14 円周率 π と自然対数の底 e が, $\mathbb{Q}$ 上代数的に独立かどうかは知られていない.

定理 2.7.1 より, 次を得る：

例 3.1.15 $k(X_1, \cdots, X_n)$ を体 k 上の n 変数有理関数体とする. $X_1, \cdots, X_n$ の基本対称式 $s_1, s_2, \cdots, s_n$ は, k 上代数的に独立である.

K/k を体の拡大とし, S を K の部分集合とする. 次を満たすとき, S を, K/k の **超越基底** という：

(1) S は k 上代数的に独立である.

(2) $K/k(S)$ は代数拡大である.

このとき, $\mathrm{card}(S)$ を K/k の **超越次数** といい, $\mathrm{trans.deg}_k(K)$ と表す. 有限個からなる超越基底が存在しないとき, K/k の超越次数は, 単に, 無限大であるともいう.

補題 3.1.27 K/k を体の拡大とし, S,T を K の部分集合とする. このとき, 次は同値である.

(1) $S \cup T$ は, k 上代数的独立である.

(2) S は, k 上代数的に独立であり, T は, $k(S)$ 上代数的に独立である.

証明 (1) $\Longrightarrow$ (2) S は, k 上代数的に独立であることは良い.

$$\{\beta_1, \cdots, \beta_n\} \subset T$$

が, $k(S)$ 上代数的に独立でないとすると, 0 でない多項式 $g(Y_1, \cdots, Y_n) \in k(S)[Y_1, \cdots, Y_n]$ が存在し, $g(\beta_1, \cdots, \beta_n) = 0$ を満たす.

$$g \in k(\alpha_1, \cdots, \alpha_m)[Y_1, \cdots, Y_n], \quad \{\alpha_1, \cdots, \alpha_m\} \subset S$$

とする. g の係数の分母を払い,

$$g(Y_1, \cdots, Y_n) = g(\alpha_1, \cdots, \alpha_m, Y_1, \cdots, Y_n) \in k[\alpha_1, \cdots, \alpha_m, Y_1, \cdots, Y_n]$$

としてよい. このとき, $g(\alpha_1, \cdots, \alpha_m, beta_1, \cdots, \beta_n) = 0$ となり, $\{\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n\}$ は, k 上代数的に独立ではない. 従って, 仮定に反し, 不合理である. よって, T は, $k(S)$ 上代数的に独立である.
(2) $\Longrightarrow$ (1)

$$\{\alpha_1, \cdots, \alpha_m\} \subset S, \quad \{\beta_1, \cdots, \beta_n\} \subset T$$

とする. 多項式

$$g(X_1, \cdots, X_m, Y_1, \cdots, Y_n) = \sum_e F_e(X_1, \cdots, X_m) Y_1^{e_1} \cdots Y_n^{e_n} \in k[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$$

が $g(\alpha_1, \cdots, \alpha_m, beta_1, \cdots, \beta_n) = 0$ を満たすとする. $\{\beta_1, \cdots, \beta_n\}$ が $k(S)$ 上代数的に独立なので,

$$F_e(\alpha_1, \cdots, \alpha_m) = 0 \quad (\forall e = (e_1, \cdots, e_n)).$$

すると, $\{\alpha_1, \cdots, \alpha_m\}$ が k 上代数的に独立なので,

$$F_e(X_1, \cdots, X_m) = 0 \quad (\forall e = (e_1, \cdots, e_n)).$$

従って, $g(X_1, \cdots, X_m, Y_1, \cdots, Y_n) = 0$ となり,

$$\{\alpha_1, \cdots, \alpha_m, beta_1, \cdots, \beta_n\}$$

は, k 上代数的に独立である. □

定理 3.1.28 K/k を体の拡大とする.

(1) $S_0(\subseteq K)$ を代数的に独立な集合とし, $S_0 \subseteq T(\subseteq K)$ を満たす T に対し, $K/k(T)$ が代数拡大であるとする. このとき, $S_0 \subseteq S \subseteq T$ を満たす, 超越基底 S を K/k は持つ.

(2) S, T を K/k の二つの超越基底とすると, $\mathrm{card}(S) = \mathrm{card}(T)$.

証明 (1) K/k は代数拡大でないとしてよい. k 上代数的に独立な, K の部分集合で, S_0 を含み T に含まれるもの全体のなす集合を $\mathcal{S}$ とする. 包含関係により順序を定めると, $(\mathcal{S}, \subseteq)$ は空でない帰納的順序集合になる. 従って, Zorn の補題により, $\mathcal{S}$ には極大元 S が存在する. T の任意の元が, $k(S)$ 上代数的なら, $K/k(S)$ が代数的となり, 証明を終わる. $x \in T - S$ が $k(S)$ 上超越的とすると, 前補題により, $S \cup \{x\}$ は, k 上代数的に独立となり, S の極大性に反する.

(2) $\mathrm{card}(S) = n$ が有限のとき, n に関する帰納法で示す. $n = 0$ のとき, T も空集合となり, 主張は正しい. $n \geq 1$ とし, $S = \{\alpha_1, \cdots, \alpha_n\}$ とする. $\beta_1 \in T$ を任意に取ると, $K/k(\beta_1, \alpha_1, \cdots, \alpha_n)$ は代数拡大である. よって, (1) より, 適当に順番を換え, $\{\beta_1, \alpha_i, \cdots, \alpha_n\}$ が超越基底としてよい. このとき, $i \geq 2$ であることに注意する. 従って, $\{\alpha_i, \cdots, \alpha_n\}$ は, $K/k(\beta_1)$ の超越基底である. また, $T - \{\beta_1\}$ も, $K/k(\beta_1)$ の超越基底である. 従って, 帰納法の仮定により,

$$n - i + 1 = \mathrm{card}(T - \{\beta_1\}).$$

よって, $|T| \leq n$. もし, $|T| < n$ ならば, 上の議論により, $|S| \leq |T| < n$ となり, 不合理である.

次に, S は無限集合とし, $S = \{\alpha_i\}_{i \in I}, T = \{\beta_j\}_{j \in J}$ とする. 任意の α_i に対し, 空でない有限部分集合 $J(i) \subset J$ が存在し, α_i は, $k(\{\beta_j \mid j \in J(i)\})$ 上代数的である. このとき, $\cup_{i \in I} J(i)$ は, K/k の超越基底である. よって

$$J = \cup_{i \in I} J(i).$$

同様にして,

$$I = \cup_{j \in J} I(j)$$

と表される. 特に, I が無限集合なので, J も無限集合である.

濃度の計算すると,

$$\mathrm{card}(J) = \mathrm{card}(\cup_{i \in I} J(i)) \leq \mathrm{card}(I)\aleph_0 \leq \mathrm{card}(I)^2 = \mathrm{card}(I).$$

J も無限集合なので, 同様にして, $\mathrm{card}(I) \leq \mathrm{card}(J)$. よって,

$$\mathrm{card}(S) = \mathrm{card}(I) = \mathrm{card}(J) = \mathrm{card}(T)$$

を得る. □

3.2 体の埋め込みとその拡張

3.2.1 定義と基本的事項

体から環への環射, 特に, 体から体への環射は常に単射となる（補題 **??**）ので, 斯かる写像を **埋め込み** ということにする.

定義 3.2.1

$$\sigma : k \longrightarrow L$$

を体 k から L への埋め込みとする. 拡大 K/k に対し,

$$\mathrm{Emb}_\sigma(K, L) = \{\tau : K \longrightarrow L \mid \tau \text{ は埋め込みで, } \tau|_k = \sigma\}$$

と表す. $\mathrm{Emb}_\sigma(K, L)$ の元 τ を, K から L への σ **上の埋め込み** という. τ が同型射のとき, σ **上の同型射** という.

特に, $\sigma(a) = a$ $(\forall a \in k)$ が成り立つとき, $\mathrm{Emb}_\sigma(K, L)$ を, $\mathrm{Emb}_k(K, L)$ と表し, その元を k **上の埋め込み** という. また, τ が同型射のとき, k **上の同型射** という. 更に, K から K への同型射を K の **自己同型射** といい, その全体を $\mathrm{Aut}(K)$ と表し, K から K への k 上の自己同型射の全体を $\mathrm{Aut}(K/k)$ と表す. $\mathrm{Aut}(K)$ は群をなし, $\mathrm{Aut}(K/k)$ はその部分群であり, $\mathrm{Aut}(K/k) \subseteq \mathrm{Emb}_k(K, K)$ が成り立つ.

問 3.2.2 K/k を体の拡大とするとき, $\mathrm{Aut}(K/k)$ が群をなすことを確かめよ.

問 3.2.3 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ を求めよ.

補題 3.2.4 K/k を代数拡大とするとき, $\mathrm{Aut}(K/k) = \mathrm{Emb}_k(K, K)$ が成り立つ.

証明 $\mathrm{Aut}(K/k) \supseteq \mathrm{Emb}_k(K, K)$ を示せばよい. τ を右辺から任意に取る. τ は単射であるので, 全射であることを示せば良い. α を K の任意の元とし, $f(X)$ を, α の k 上の最小多項式とする. K' を $f(X) = 0$ の根で K に含まれるもの全てを k に添加して得られた体とする. すると K' は K に含まれ, $[K' : k]$ は有限である. τ は $f(X)$ の根をまた $f(X)$ の根に移すので, τ を K' に制限した写像の像 $\tau(K')$ は K' に含まれる. τ の定義域, 値域を K' に制限した写像も τ で表す. 環射 $\tau : K' \rangle K'$ は, 特に, k 上ベクトル空間の単射線形写像である. $\dim_k K' = [K' : k]$ は有限なので, $\tau : K' \longrightarrow K'$ は全射となる. 従って $\tau(\beta) = \alpha$ となる $\beta \in K' \subseteq K$ が存在し, $\tau \colon K \longrightarrow K$ は全射である. □

$\sigma : k \longrightarrow L$ を埋め込みとする. k 係数多項式 $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in k[X]$ に対し,

$$f^\sigma(X) = \sigma(a_n) X^n + \cdots + \sigma(a_1) X + \sigma(a_0) \in L[X]$$

と定める.

補題 3.2.5 $\sigma : k \longrightarrow \Omega$ を体 k から代数閉体 Ω への埋め込みとする. $k(\alpha)/k$ を代数拡大とし, $f(X)$ を α の最小多項式とする. $f^\sigma(X)$ の相異なる根全体の集合を $R(f^\sigma)$ と表す. このとき,

$$\phi : \mathrm{Emb}_\sigma(k(\alpha), \Omega) \longrightarrow R(f^\sigma); \quad \tau \longmapsto \tau(\alpha)$$

は全単射である.

特に, $|\mathrm{Emb}_\sigma(k(\alpha), \Omega)| \leq \deg(f)$.

証明 $f(\alpha)=0$ なので, $\tau\in \mathrm{Emb}_\sigma(k(\alpha),\Omega)$ に対し, $f^\sigma(\tau(\alpha))=0$. 従って, $\tau(\alpha)\in R(f^\sigma)$. また, $\tau(\alpha)$ が τ を定めるので, ϕ は単射である. $\beta\in R(f^\sigma)$ に対し, 環射

$$\tilde{\tau}: k[X]\longrightarrow \Omega,\quad g(X)\longmapsto g^\sigma(\beta)$$

を考える. $f(X)\in \mathrm{Ker}(\tilde{\tau})$ なので, $(f(X))\subseteq \mathrm{Ker}(\tilde{\tau})\subsetneq k[X]$. $(f(X))$ は極大イデアルなので, $(f(X))=\mathrm{Ker}(\tilde{\tau})$. 従って, $\tilde{\tau}$ は, σ 上の埋め込み

$$\tau: k(\alpha)\simeq k[X]/(f(X))\longrightarrow (\sigma(k))(\beta)\subseteq\Omega$$

を導き, $\phi(\tau)=\tau(\alpha)=\beta$. よって, ϕ は全射である. □

例 3.2.1 $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式は X^4-2 であり,

$$X^4-2=(X-\sqrt[4]{2})(X-i\sqrt[4]{2})(X+\sqrt[4]{2})(X+i\sqrt[4]{2})\in\mathbb{C}[X].$$

$$\begin{array}{lccc}\sigma_1: & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}\\ \sigma_2: & \sqrt[4]{2} & \longmapsto & i\sqrt[4]{2}\\ \sigma_3: & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2}\\ \sigma_4: & \sqrt[4]{2} & \longmapsto & -i\sqrt[4]{2}\end{array}$$

とするとき,

$$\mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}),\mathbb{C})=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}.$$

また, $\sqrt[4]{2}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式は $X^2-\sqrt{2}$ であり,

$$X^2-\sqrt{2}=(X-\sqrt[4]{2})(X+\sqrt[4]{2}).$$

$$\mathrm{Emb}_{\mathbb{Q}(\sqrt{2})}(\mathbb{Q}(\sqrt[4]{2}),\mathbb{C})=\{\sigma_1,\sigma_3\}.$$

定理 3.2.6 (埋め込みの延長可能定理) K/k を代数拡大とし, $\sigma: k\longrightarrow\Omega$ を, k の代数閉体 Ω への埋め込みとする. このとき,

$$\mathrm{Emb}_\sigma(K,\Omega)\neq\emptyset.$$

証明 K/k の中間体 F と σ 上の埋め込み $\tau: F\longrightarrow\Omega$ の組 (F,τ) 全体のなす集合を $\mathcal{S}$ とする. $(k,\sigma)\in\mathcal{S}$ なので $\mathcal{S}$ は空集合ではない. $(F,\tau),(E,\mu)\in\mathcal{S}$ に対し

$$(F,\tau)\leq(E,\mu)\quad\overset{\mathrm{def}}{\Longleftrightarrow}\quad F\subseteq E,\ \mu|_F=\tau$$

と定めると, $\mathcal{S}$ は順序集合となる. $\mathcal{S}$ は帰納的順序集合であることを示す.

$\mathcal{T}=\{(F_i,\tau_i)|i\in I\}$ を $\mathcal{S}$ の全順序部分集合とする. このとき $F=\cup F_i$ は K/k の中間体である. σ の F への拡張を次のように定める.

$$\tau(\alpha)=\tau_i(\alpha),\quad \alpha\in F_i.$$

すると (F,τ) は $\mathcal{T}$ の上限である. 従って $\mathcal{S}$ は帰納的順序集合であることがわかった. よって, Zorn の補題により, $\mathcal{S}$ には極大元 (E,μ) が存在する.

$E \neq K$ とすると, E に含まれない K の元 α が存在する. $E(\alpha)/E$ は代数拡大なので, 補題 3.2.5 により, μ の $E(\alpha)$ への拡張 ν が存在する. このとき $(E(\alpha), \nu) \in \mathcal{S}$ であり, (E, μ) より真に大きい. これは (E, μ) の極大性に反する. 従って $E = K$ となり, σ の K への拡張 μ が得られた. □

この定理を利用して, 体 k の代数閉包の一意性を示そう.

系 3.2.7 （代数閉包の一意性）$\sigma : k \longrightarrow k'$ を体の同型射とし, E, E' を体 k, k' の代数閉包とする. このとき σ 上の同型射 $E \longrightarrow E'$ が存在する.

証明 $\sigma : k \longrightarrow k'$ と, 自然な埋め込み $k' \longrightarrow E'$ の合成射も σ と表すことにする. 定理により σ 上の埋め込み $\tau : E \longrightarrow E'$ が存在することがわかる. E が代数閉体なので, $\sigma(E)$ も代数閉体であり, k' 上代数的である. $E'/\sigma(E)$ は代数拡大であるから $E' = \sigma(E)$. 従って, $\sigma : E \longrightarrow E'$ は, σ 上の同型射である. □

例 3.2.2 t を変数とする一変数有理関数体 $\mathbb{F}_p(t)$ を考える. X を新たな変数とするとき, 多項式 $X^p - t \in \mathbb{F}_p(t)[X]$ は, $\mathbb{F}_p(t)$ 上既約多項式である. Ω を $\mathbb{F}_p(t)$ の代数閉包とし, $\alpha \in \Omega$ を $X^p - t = 0$ の根とする. このとき,

$$X^p - t = (X - \alpha)^p$$

と因数分解され,

$$\mathrm{Emb}_{\mathbb{F}_p(t)}(\mathbb{F}_p(t)(\alpha), \Omega) = \{id_{\mathbb{F}_p(t)(\alpha)}\}.$$

補題 3.2.8 K/k を有限次代数拡大とし $\sigma : k \longrightarrow \Omega$ を体 k から代数閉体 Ω への埋め込みとする. このとき,

$$|\mathrm{Emb}_\sigma(K, \Omega)|$$

は代数閉体 Ω と埋め込み σ の取り方によらない.

証明 $\sigma' : k \longrightarrow \Omega'$ も k から代数閉体 Ω' への埋め込みとする. L, L' をそれぞれ $\sigma(k), \sigma'(k)$ の Ω, Ω' に含まれる代数閉包とする. このとき, L, L' は, $\sigma(k), \sigma'(k)$ の代数閉包である. また,

$$\mathrm{Emb}_\sigma(K, L) = \mathrm{Emb}_\sigma(K, \Omega), \quad \mathrm{Emb}_{\sigma'}(K, L') = \mathrm{Emb}_{\sigma'}(K, \Omega')$$

が成り立つことに注意する.

さて, 代数閉包の一意性（系 3.2.7）により

$$\sigma' \circ \sigma^{-1} : \sigma(k) \longrightarrow \sigma'(k)$$

上の同形射

$$\phi : L \longrightarrow L'$$

が存在する. 二つの写像

$$\begin{aligned} \xi : \mathrm{Emb}_\sigma(K, L) \quad &; \quad \tau \longmapsto \phi \circ \tau, \\ \eta : \mathrm{Emb}_{\sigma'}(K, L') \quad &; \quad \tau' \longmapsto \phi^{-1} \circ \tau' \end{aligned}$$

は, 互いに他の, 逆写像なので, ξ, η は全単射であり,

$$\mathrm{Emb}_\sigma(K, L) \simeq \mathrm{Emb}_{\sigma'}(K, L').$$

よって,

$$|\mathrm{Emb}_\sigma(K,\Omega)| = |\mathrm{Emb}_{\sigma'}(K,\Omega')|$$

が成り立つ. □

3.2.2 最小分解体と正規拡大

定義 3.2.9 k を体とし, $f(X) \in k[X]$ を次数が n (≥ 1), 最高次係数が 1 の多項式とする. L を k の代数閉包とし,

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$$

を $L[X]$ に於ける因数分解とする. このとき,

$$K = k(\alpha_1, \cdots, \alpha_n)$$

を f の k 上の（L における）**最小分解体** という.

例 3.2.3 $\mathbb{Q}(\sqrt{a^2-4b})$ は $X^2+aX+b \in \mathbb{Q}[X]$ の（$\bar{\mathbb{Q}}$ における）最小分解体である.

例 3.2.4 X^3-2 の $\mathbb{Q}$ 上の（$\bar{\mathbb{Q}}$ における）最小分解体 K は, ω を 1 の虚数立方根とするとき $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ であり, $[K:\mathbb{Q}] = 6$ である.

問 3.2.10 n 次式 $f(X) \in k[X]$ の最小分解体を K とするとき, $[K:k] \leq n!$ を示せ.

定理 3.2.11 （最小分解体の一意性定理）k を体とし $f(X) \in k[X]$ $(\deg(f) \geq 1)$ とする. f の最小分解体は, k 上の同型を除いて, 一意的に定まる.

証明 L, L' を k の代数閉包とすると, 補題 3.1.20 (4) により, $f(X)$ は, $L[X], L'[X]$ において一次式の積に因数分解される:

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_n),$$
$$f(X) = (X-\beta_1)\cdots(X-\beta_n)$$

と因数分解される. そこで,

$$K = k(\alpha_1, \cdots, \alpha_n), \quad K' = k(\beta_1, \cdots, \beta_n)$$

とおく. すると, K, K' は, $f(X)$ の最小分解体である. L, L' は, 共に k の代数閉包であり, 系 3.2.7 により, k 上の同型 $\tau : L \longrightarrow L'$ が存在する. このとき,

$$f(X) = (X-\tau(\alpha_1))\cdots(X-\tau(\alpha_n)) \in L'[X]$$

であり, $L'[X]$ に於ける因数分解は一意的なので,

$$\{\beta_1, \cdots, \beta_n\} = \{\tau(\alpha_1), \cdots, \tau(\alpha_n)\}.$$

よって, $K' = \tau(K)$ となり, K と K' は, k 上同型である. □

定理 3.2.12 K/k を代数拡大とするとき次は同値である.

(1) $k[X]$ の既約多項式は K に根をもつならば, K に於て一次式の積に因数分解される,

(2) K の代数閉包は, k の代数閉包でもあるので, それを $\bar{k}$ と表す. このとき, $\mathrm{Emb}_k(K,\bar{k}) = \mathrm{Aut}(K/k)$ が成り立つ,

(3) K を含む k の任意の代数閉包 $\bar{k}$ に対し, $\sigma(K) = K$ $(\forall\sigma \in \mathrm{Aut}(\bar{k}/k))$,

(4) K を含む k の一つの代数閉包 $\bar{k}$ とするとき, $\sigma(K) = K$ $(\forall\sigma \in \mathrm{Aut}(\bar{k}/k))$.

これらの条件を満たす拡大を **正規拡大** という.

証明 (1) $\Longrightarrow$ (2) $\mathrm{Aut}(K/k) \subseteq \mathrm{Emb}_k(K,\bar{k})$ なので, 逆の包含関係を示す. $\sigma \in \mathrm{Emb}_k(K,\bar{k})$ を任意にとる. $\alpha \in K$ の k 上の最小多項式を f とすると, 仮定より f は $K[X]$ に於て一次式の積に因数分解される. すると $\sigma(\alpha)$ もまた $f(X)$ の根であるから $\sigma(\alpha) \in K$ である. α は任意であったから, $\sigma(K) \subseteq K$. 補題 3.2.4 により, $\sigma(K) = K$ を得て, $\sigma \in \mathrm{Aut}(K/k)$.
(2) $\Longrightarrow$ (3) $\sigma \in \mathrm{Aut}(\bar{k}/k)$ ならば, $\sigma|_K \in \mathrm{Emb}_k(K,\bar{k})$. (2) より, $\sigma(K) = K$.
(3) $\Longrightarrow$ (4) は自明であり, (4) $\Longrightarrow$ (1) を示す. 既約多項式 $f(X) \in k[X]$ が K に於て, 根 α を持ったとする. すると f は α の k 上の最小多項式である. f の任意の根 β に対し, 補題 3.2.5 により, k 上の埋め込み $\sigma \in \mathrm{Emb}_k(k(\alpha),\bar{k})$ で $\sigma(\alpha) = \beta$ となるものが存在する. 定理 3.2.6 により, σ の $\bar{k}$ への拡張が存在する. それも σ で表す. (4) より $\sigma(K) = K$. 特に, $\sigma(\alpha) = \beta \in K$. 従って $f(X)$ の任意の根は K に含まれる. □

例 3.2.5 体 k の代数閉包を $\bar{k}$ とするとき, $\bar{k}/k$ は正規拡大である.

定理 3.2.13 K/k を体の拡大とするとき, 次は同値である.

(1) K/k は有限次正規拡大である.

(2) K はある多項式 $f(X) \in k[X]$ の最小分解体である.

証明 (1) $\Longrightarrow$ (2) $[K:k]$ は有限なので, $K = k(\alpha_1,\cdots,\alpha_n)$ と表される. 各 α_i の k 上の最小多項式を $f_i(X)$ とし, $f = f_1\cdots f_n$ とする. f_i は既約多項式で, K において根を持つ. 定理 3.2.12 により, f_i は $K[X]$ において一次式の積に分解する. 従って $f(X)$ も $K[X]$ において一次式の積に分解し, $f(X) = 0$ の根すべてを k に添加して得られる体は K に等しい. よって K は $f(X)$ の k 上の最小分解体である.
(2) $\Longrightarrow$ (1) K を $f(X) \in k[X]$ の最小分解体とすると, K/k は有限次拡大である.

$$f(X) = (X-\alpha_1)\cdots(X-\alpha_n) \in K[X]$$

とすれば, 定義から, $K = k(\alpha_1,\cdots,\alpha_n)$ である. $\bar{k}$ を K を含む k の代数閉包とするとき, $\sigma \in \mathrm{Emd}_k(K,\bar{k})$ に対し,

$$\prod_{i=1}^{n}(X-\alpha_i) = f(X) = f^{\sigma}(X) = \prod_{i=1}^{n}(X-\sigma(\alpha_i))$$

なので

$$\{\alpha_1, \cdots, \alpha_n\} = \{\sigma(\alpha_1), \cdots, \sigma(\alpha_n).\}$$

従って $\sigma(K) = K$. 再び, 定理 3.2.12 より, K/k は正規拡大である. □

例 3.2.6 K/k を二次拡大とし, $\alpha \in K - k$ とする. α の k 上の最小多項式を $f(X) = X^2 + aX + b$ とし, その根を, α, β とする. このとき, $\beta = -a - \alpha$ なので, $K = k(\alpha) = k(\alpha, \beta)$ は, $f(X) \in k[X]$ の最小分解体である. 従って, 二次拡大は常に正規拡大である.

例 3.2.7 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ は共に正規拡大であるが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大でない. すなわち, 正規拡大を二つ重ねたものは, 一般には正規拡大ではない.

補題 3.2.14 (1) K, F を体 L の部分体とする.

$$K/k : \text{正規拡大}, \ F/k : \text{任意の拡大} \quad \Longrightarrow \quad KF/F : \text{正規拡大}.$$

(2) $K \supseteq E \supseteq k$ を体の列とする.

$$K/k : \text{正規拡大} \quad \Longrightarrow \quad K/E : \text{正規拡大}.$$

(3) K_1, K_2 を体 L の部分体とする.

$$K_1/k, K_2/k : \text{正規拡大} \quad \Longrightarrow \quad K_1K_2/k, \ (K_1 \cap K_2)/k : \text{正規拡大}.$$

証明 (1) $\bar{F}$ を F の代数閉包とし, $\sigma : KF \longrightarrow \bar{F}$ を F 上の任意の埋め込みとする. K/k は正規拡大なので $\sigma(K) = K$. 従って $\sigma(KF) = KF$ となり, 定理 3.2.12 により KF/F が正規拡大であることを知る. (2) K を含む E の代数閉包を $\bar{E}$ とし, $\sigma \in \mathrm{Aut}(\bar{E}/E))$ をとる. このとき, $\sigma \in \mathrm{Aut}(\bar{E}/k))$ であり, K/k は正規拡大なので, $\sigma(K) = K$ が成り立つ. 従って, 定理 3.2.12 により, K/E は正規拡大である. (3) K_1K_2 を含む k の代数閉包を $\bar{k}$ とし, $\sigma \in \mathrm{Aut}(\bar{k}/k))$ をとる. $K_1/k, K_2/k$ は正規拡大なので, $\sigma(K_i) = K$ が成り立ち, $\sigma(K_1K_2) = K_1K_2, \sigma(K_1 \cap K_2) = K_1 \cap K_2$ が成り立つ. 従って, 定理 3.2.12 により, $K_1K_2/k, K_1 \cap K_2/k$ は正規拡大である. □

補題 3.2.15 (最小正規拡大の存在) E/k を有限次拡大とし, E を含む k の代数閉包を $\bar{k}$ とする. $\mathrm{Emb}_k(E, \bar{k}) = \{\sigma_1, \cdots, \sigma_n\}$ とし,

$$K = \sigma_1(E) \cdots \sigma_n(E)$$

とする. このとき K/k は E を含む最小の正規拡大である.

証明 $\tau : K \longrightarrow \bar{k}$ を k 上の任意の埋め込みとすると

$$\{\tau\sigma_1, \cdots, \tau\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$$

となり, $K = \tau(K)$. 従って K/k は正規拡大である.

正規拡大 F/k に対し, $E \subset F$ ならば, $\sigma_i : E \longrightarrow \bar{k}$ の F への延長も σ_i と表すとき, $\sigma_i(E) \subseteq \sigma_i(F) = F$ が成り立ち, $K \subseteq F$ を得る. □

3.3 分離拡大

K/k を代数拡大とするとき, $\alpha \in K\backslash k$ の k 上の最小多項式 $f(X)$ は $\deg(f) \geq 2$ を満たす. $\mathrm{char}(k) = 0$ ならば, $f' \neq 0$ であり, $\deg(f') < \deg(f)$. 従って, $f'(\alpha) \neq 0$ であり, α は, $f(X)$ の重根ではない. しかし, $\mathrm{char}(k) = p > 0$ のとき, 最小多項式 $f(X)$ が重根を持つ場合が有る. この様な状況が生ずるのは, 特別な場合であり, その理解には新しい概念を必要とする.

3.3.1 多項式の微分と分離多項式

k を体とし, 多項式 $f(X) \in k[X]$ が

$$f(X) = (X-\alpha)^e g(X), \quad (\alpha \in k,\ g(X) \in k[X])$$

と因数分解され, $g(\alpha) \neq 0$ のとき, α を多項式 $f(X)$ の e **重根** といい, $e \geq 2$ のとき, 単に, 重根という.

多項式が重根を持つかどうかを判定するために, 多項式の微分を考える. 一般の体で微分を考えるので少し注意が必要である.

k を体とする. 写像

$$\mathbb{Z} \longrightarrow k, \quad n \longmapsto n \cdot 1$$

により, k は $\mathbb{Z}$-加群となることを思い出す. すなわち, スカラー倍

$$\mathbb{Z} \times k \longrightarrow k, \quad (n, a) \longmapsto n \cdot a = (n \cdot 1)a$$

が定義される. 以下, $n \cdot a = na$ と略記する.

多項式

$$f(X) = a_0 + a_1 X + \cdots a_n X^n \ \in k[X]$$

に対し

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$$

を $f(X)$ の **微分** という. 上で注意したことから, $f'(X)$ は k 係数多項式である.

例 3.3.1 $f(X) = X^p - 1 \in \mathbb{F}_p[X]$ とするとき, $f'(X) = 0$.

次の補題は, 容易に確かめられる：

補題 3.3.1 体 k 上の一変数多項式の微分について, 次が成り立つ:

(1) $c' = 0$ $(c \in k)$,

(2) $(f+g)' = f' + g'$,

(3) $(fg)' = f'g + fg'$.

問 3.3.2 上の補題を確かめよ.

補題 3.3.3 k を体とし, $f(X) \in k[X]$ とする. $\alpha \in k$ に対し

$$\alpha \text{ は } f(X) \text{ の重根} \quad \Longleftrightarrow \quad f(\alpha) = f'(\alpha) = 0.$$

証明 $f(X)$ が重根 α を持つと

$$f(X) = (X-\alpha)^2 g(X)$$

と因数分解される. すると

$$f'(X) = 2(X-\alpha)g(X) + (X-\alpha)^2 g'(X)$$

となり, $f(\alpha) = f'(\alpha) = 0$. 逆に $f(\alpha) = f'(\alpha) = 0$ とする. すると, $f(X) = (X-\alpha)g(X)$ と因数分解され, $f'(X) = g(X) + (X-\alpha)g'(X)$ と表される. 従って, $g(\alpha) = 0$ となり, $g(X) = (X-\alpha)h(X)$ と因数分解され, $f(X) = (X-\alpha)^2 k(X)$ と表される. よって, α は $f(X)$ の重根である. □

定義 3.3.4 k を体とし, $f(X) \in k[X]$ とする. f の各既約因子が重根を持たないとき, f を **分離多項式** という. k 上代数的な元 α の最小多項式が分離多項式のとき, α は k 上 **分離代数的である** という.

例 3.3.2 k を正標数 p の体とし, n を p と互に素な正整数とする. このとき k 係数多項式 $X^n - a$ $(a \in k^\times)$ は分離多項式である.

一方, $f(X) = X^p - a$ $(a \in k^\times)$ は分離多項式でない. 実際, $X^p - a = (X - \sqrt[p]{a})^p$ と因数分解され, $\sqrt[p]{a}$ は p 重根である.

補題 3.3.5 k を体とし, $f(X) \in k[X]$ を既約多項式とする. このとき, 次は同値である:

(1) $f(X)$ は分離多項式.

(2) $f'(X) \neq 0$.

特に, $\mathrm{char}(k) = 0$ ならば, 既約多項式 $f(X)$ は重根を持たない.

証明 $f(X)$ が分離多項式でないとする. 即ち, $f(X)$ が重根 α を持つとする. このとき, $f(X)$ は α の最小多項式であり, $f'(\alpha) = 0$ を満たす. 従って $f'(X) = 0$ である. 逆に $f'(X) = 0$ とする. $f(\alpha) = 0$ とすると, $f'(\alpha) = 0$ なので, 補題 3.3.3 により, α は $f(X)$ の重根である. □

3.3.2 分離代数拡大

定義 3.3.6 K/k を代数拡大とする. K の全ての元が k 上分離代数的のとき K/k を **分離代数拡大** という.

例 3.3.3 $\mathrm{char}(k) = 0$ ならば, 任意の代数拡大 K/k は分離的である.

定義 3.3.7 K/k を有限次代数拡大とし $\sigma : k \longrightarrow \Omega$ を体 k から代数閉体 Ω への埋め込みとする.

$$[K : k]_s := |\mathrm{Emb}_\sigma(K, \Omega)|$$

を拡大 K/k の **分離次数** という. 分離次数は, 補題 3.2.8 により, 代数閉体 Ω と埋め込み $\sigma : k \longrightarrow \Omega$ の取り方によらない.

補題 3.3.8 K/k を有限次代数拡大とする. このとき次が成り立つ：

(1) K/k の中間体 F に対し, $[K:k]_s = [K:F]_s[F:k]_s$,

(2) $[K:k]_s \leq [K:k]$,

(3) $[K:k] = [K:k]_s$ ならば, 任意の中間体に対し, $[F:k] = [F:k]_s$.

証明 (1) K を含む k の代数閉包を $\bar{k}$ とし,

$$\mathrm{Emb}_k(F, \bar{k}) = \{\sigma_1, \cdots, \sigma_r\}, \quad r = [F:k]_s$$

とする. 補題 3.2.8 により, $\mathrm{Emb}_{\sigma_i}(K, \bar{k})$ に含まれる個数は i によらず $[K:F]_s$ に等しい. 従って $[K:k]_s = [K:F]_s[F:k]_s$.
(2) K/k は有限次拡大なので, $K = k(\alpha_1, \cdots, \alpha_n)$ と表せる. $K_i := k(\alpha_1, \cdots, \alpha_i)$ とすると, $K_i = K_{i-1}(\alpha_i)$. 補題 3.2.5 により, $[K_i(\alpha_{i+1}) : K_i]_s \leq [K_i(\alpha_{i+1}) : K_i]$. 従って (1) より (2) を得る. (3) は, (1) と (2) から, 直ちに得られる. □

補題 3.3.9 K/k を代数拡大とし, $\alpha \in K$ とする. このとき, 次は同値である:

(1) α が k 上分離代数的である,

(2) $[k(\alpha):k]_s = [k(\alpha):k]$,

(3) $k(\alpha)/k$ は分離代数拡大である.

証明 K を含む k の代数閉包を $\bar{k}$ とする. $f(X)$ を α の k 上の最小多項式とすると, 補題 3.2.5 により, $f(X)$ が分離多項式であるための条件は, $[k(\alpha):k]_s = [k(\alpha):k]$. 即ち, (1) $\Longleftrightarrow$ (2) を得る. 任意の $\beta \in k(\alpha)$ に対し, (2) を仮定すれば, 補題 3.3.8 より, $[k(\beta):k]_s = [k(\beta):k]$ を得る. 上で示したことより, β は, k 上分離代数的である. よって, (3) を得る. (3) $\Longrightarrow$ (1) は明らか. □

補題 3.3.10 K/k を代数拡大とし, K の部分集合 S の各元が k 上分離代数的とする. このとき, $k(S)/k$ は分離代数拡大である.

証明 任意の $\alpha \in k(S)$ が k 上分離的であることを示そう. 明らかに S の有限部分集合 $\{\alpha_1, \cdots, \alpha_n\}$ が存在して

$$\alpha \in k(\alpha_1, \cdots, \alpha_n).$$

$$K_0 := k, \quad K_i := k(\alpha_1, \ldots, \alpha_i) \quad (i = 1, \cdots, n)$$

とすると, 各 i に対し, α_i は, K_{i-1} 上分離代数的なので, 補題 3.3.9 より, $[K_i : K_{i-1}]_s = [K_i : K_{i-1}]$. 従って, 補題 3.3.8 より, $[K_n : k]_s = [K_n : k]$ が成り立ち, 更に, $[k(\alpha):k] = [k(\alpha):k]_s$ が成立つ. よって, 補題 3.3.9 より, α は k 上分離的である. □

定理 3.3.11 K/k を有限次拡大とする. このとき次は同値である.

(1) K/k は, 有限次分離代数拡大である.

(2) $[K:k]_s = [K:k]$.

証明 (1) $\Longrightarrow$ (2) K/k は有限次拡大なので,

$$k \subseteq K_1 := k(\alpha_1) \subseteq \cdots \subseteq K_n := k(\alpha_1, \cdots, \alpha_n) = K$$

となる K の元 α_i $(1 \leq i \leq n)$ が存在する. α_{i+1} は, K_i 上分離代数的なので, 補題 3.3.9 より, $[K_i(\alpha):K_i]_s = [K_i(\alpha):K_i]$. 従って, 補題 3.1.6 と補題 3.3.8 より, (2) を得る. 逆に (2) を仮定すれば, 補題 3.3.8 より, 任意の $\alpha \in K$ に対し, $[k(\alpha):k]_s = [k(\alpha):k]$. 従って, 補題 3.3.9 より, α は k 上分離代数的である. □

補題 3.3.12 (1) $k \subseteq F \subseteq K$ を体の列とする. このとき

$$K/k : \text{分離代数拡大} \quad \Longleftrightarrow \quad K/F, F/k : \text{分離代数拡大}.$$

(2) K, F は体 L の部分体で体 k を含むとする.

$$K/k : \text{分離代数拡大} \quad \Longrightarrow \quad KF/F : \text{分離代数拡大}.$$

(3) E, F を体 L の部分体とする.

$$E/k, F/k : \text{分離代数拡大} \quad \Longrightarrow \quad EF/k : \text{分離代数拡大}.$$

証明 (1) $\Longrightarrow$ は明らかなので, $\Longleftarrow$ を示す. $\alpha \in K$ を任意にとる. α の F 上の最小多項式 $f(X) = X^n + \beta_1 X^{n-1} + \cdots + \beta_n$ は, 分離多項式である. $F_1 = k(\beta_1, \cdots, \beta_n)$ とすると, 各 β_i が k 上分離代数的なので, 補題 3.3.10 により, F_1/k は有限次分離代数拡大である. 一方 $F_1(\alpha)/F_1$ も分離代数拡大である. 従って, 補題 3.3.8 と 定理 3.3.11 により

$$[F_1(\alpha):k] = [F_1(\alpha):F_1][F_1:k] = [F_1(\alpha):F_1]_s[F_1:k]_s = [F_1(\alpha):k]_s.$$

従って, 定理 3.3.11 より, α は k 上分離的である.
(2) $\alpha \in KF$ を任意にとると

$$\alpha = \frac{a_1b_1 + \cdots + a_nb_n}{c_1d_1 + \cdots + c_md_m} \quad a_i, c_j \in K,\ b_i, d_j \in F$$

と表される.

$$F_1 = F(a_1, \cdots, a_n; c_1, \cdots, c_m)$$

とすると, 各 a_i, c_j は k 上分離的なので, F 上分離的である. 従って, 補題 3.3.10 により, F_1/F は分離拡大となり, α は, F 上分離代数的である.
(3) は (1) と (2) を組合せれば良い. □

3.3.3 純非分離拡大, 分離閉包, 完全体

定理-定義 3.3.13 k を体とし, $\bar{k}$ をその代数閉包とする. $\alpha \in \bar{k}$ の最小多項式を $f(X) \in k[X]$ とする.

(1) $\mathrm{char}(k) = 0$ ならば, $f(X)$ は分離多項式である.

(2) $\mathrm{char}(k) = p > 0$ ならば, 整数 $e \geq 0$ と分離既約多項式 $g(X) \in k[X]$ が一意的に存在して

$$f(X) = g(X^{p^e}).$$

さらに, α^{p^e} は, k 上分離的であり,

$$[k(\alpha) : k] = p^e \deg g, \quad [k(\alpha) : k]_s = \deg g$$

が成り立つ.

p^e を f の **非分離次数** といい, g を f の **被約多項式** という

$f(X)$ が重根を持つならば, 補題 3.3.5 より, $f'(X) = 0$ である. $\mathrm{char}(k) = 0$ ならば, これは有り得ない. 従って (1) を得る. そこで, $\mathrm{char}(k) = p > 0$ とする. f が分離的ならば $e = 0, f = g$ とすればよい. $f(X)$ が非分離的とすると, $\deg(f) = n > 1$.

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n, \quad a_0 \neq 0$$

とすると

$$f'(X) = n a_0 X^n + (n-1) a_1 X^{n-2} + \cdots + a_{n-1} = 0.$$

すなわち

$$(n-i) a_i = 0, \quad i = 0, 1, \cdots, n-1$$

となり, $a_i \neq 0 \Longrightarrow p | i$. よって

$$f(X) = a_0 X^{pn_1} + a_p X^{p(n_1-1)} + \cdots + a_{pn_1} \quad (n = pn_1)$$

と表される.

$$f_1(X) = a_0 X^{n_1} + a_p X^{n_1-1} + \cdots + a_{pn_1}$$

とすれば $f(X) = f_1(X^p)$ であり, $f(X)$ が既約なので, $f_1(X)$ も既約である. f_1 が分離的ならばそれでおしまい. もし, f_1 が非分離的ならば上と同じ議論を f_1 に施す. これを繰返して e と分離既約多項式 $g(X)$ を得る.

$g(X) = (X - \beta_1) \cdots (X - \beta_s)$ とすると,

$$f(X) = \prod_{i=1}^{s} (X^{p^e} - \beta_i) = \prod_{i=1}^{s} (X - \gamma_i)^{p^e}.$$

但し, γ_i は $X^{p^e} = \beta_i$ の解である. 従って, 補題 3.2.5 より, $\deg g = s = [k(\alpha) : k]_s$ であり,

$$[k(\alpha) : k] = p^e [k(\alpha) : k]_s.$$

$\alpha = \gamma_1$ とすると, $\alpha^{p^e} = \beta_1$ であり, これは, k 上分離的である. □

定義 3.3.14 K/k を代数拡大とする. $\alpha \in K$ の最小多項式 $f(X)$ が

$$f(X) = X^{p^e} - a \in k[X] \quad (e \geq 0)$$

と表されるとき, 即ち, f の被約多項式が一次式のとき, α は k 上 **純非分離的** という. K の元がすべて純非分離的のとき, K/k を **純非分離代数拡大** という.

補題 3.3.15 K/k を代数拡大とし, K 含む k の代数閉包を $\bar{k}$ とする. このとき, $\alpha \in K$ に対し, 次は同値である.

(1) α は k 上純非分離的である,

(2) $\sigma(\alpha) = \alpha$ $(\forall \sigma \in \mathrm{Emb}_k(K, \bar{k}))$.

証明 (1) $\Longrightarrow$ (2) k 上純非分離的な α の最小多項式は $f(X) = X^{p^e} - a$ $(a \in k)$ と表される. k 上の埋め込み $\sigma : K \rangle \bar{k}$ に対し, $f(\alpha) = f(\sigma(\alpha)) = 0$. 従って $\alpha^{p^e} = a = (\sigma(\alpha))^{p^e}$ となり,

$$(\alpha - \alpha^\sigma)^{p^e} = \alpha^{p^e} - \sigma(\alpha)^{p^e} = 0.$$

よって $\alpha = \alpha^\sigma$ を得る.
(2) $\Longrightarrow$ (1) $f(X) \in k[X]$ を α の最小多項式とする. このとき, f の非分離次数, 被約多項式を p^e, g とすると, 定理 3.3.13 より, $f(X) = g(X^{p^e})$. $\deg(g) \geq 2$ とすると, $f(X) = 0$ は α 以外の根 $\beta \in \bar{k}$ を持つ. すると, 補題 3.2.5 により, k 上の埋め込み $\sigma : k(\alpha) \rangle \bar{k}$ で $\sigma(\alpha) = \beta$ となるものが存在する. これは仮定に反する. 従って g は一次式となり, α は k 上純非分離的である. □

補題 3.3.8 を考慮すると, 次を得る：

系 3.3.16 K/k を代数拡大とする. このとき次は同値である.

(1) K/k は純非分離拡大である,

(2) $[K : k]_s = 1$.

定理 3.3.17 K/k を代数拡大とし, K_s を k 上分離代数的な元全体からなる K の部分集合とする. このとき K_s は, K の部分体であり, K_s/k は分離代数拡大であり, K/K_s は純非分離拡大である. K_s を K における k の **分離閉包** という.

K/k が有限次拡大ならば, $[K : k]_s = [K_s : k]$ であり,

$$[K : k]_i := [K : K_s] = [K : k]/[K : k]_s$$

は, 体の標数の冪である. $[K : k]_i$ を拡大 K/k の **非分離次数** という.

証明 $\mathrm{char}(k) = 0$ ならば, 証明すべきことがない. そこで, $\mathrm{char}(k) = p > 0$ とする. $\alpha, \beta \in K_s$ に対し, 補題 3.3.10 より, $k(\alpha, \beta)/k$ は有限次分離代数拡大である. 従って, $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ $(\alpha \neq 0)$ は全て, k 上分離的となり, K_s は体をなす. 明らかに, K_s/k は分離代数拡大である. K の任意の元 α に対し, 定理 3.3.13 より, α^{p^e} が, k 上分離代数的となる $e \geq 0$ が存在する. 従って, α の K_s

上の最小多項式は, $X^{p^e} - \alpha^{p^e}$ の約数となり, α のみを根に持つ. 従って, α は K_s 上純非分離的である.

K/k を有限次拡大とする. 補題 3.3.8, 補題 3.3.16, 定理 3.3.11 等より,

$$[K : k]_s = [K : K_s]_s[K_s : k]_s = [K_s : k]_s = [K_s : k]$$

が成り立つ. K/K_s は有限次拡大なので,

$$K_0 = K_s \subset K_1 := K_0(\alpha_1) \subseteq \cdots \subseteq K_n := K_{n-1}(\alpha_n) = K$$

となる, $\alpha_i \in K$ が存在する. α_i は, k 上純非分離的なので, K_{i-1} 上純非分離的であり, $[K_i : K_{i-1}] = p^{e_i}$ となる $e_i \geq 0$ が存在する. 従って,

$$[K : k]_i = [K : K_s] = \prod_{i=1}^{n} [K_i : K_{i-1}] = p^{e_1 + \cdots + e_n}$$

が成り立つ. □

問 3.3.18 $L/K, K/k$ を有限次拡大とする. このとき,

$$[L : k]_i = [L : K]_i[K : k]_i$$

が成り立つことを確かめよ.

系 3.3.19 K/k を有限次拡大とし, $[K : k]_i = p^e$ とする. このとき, $\alpha \in K$ に対し, α^{p^e} は k 上分離的である.

証明 $[k(\alpha) : k]_i = p^{e'}$ は $[K : k] = p^e$ の約数である. $\alpha^{p^{e'}}$ は k 上分離的なので, α^{p^e} も k 上分離的である. □

定理 3.3.20 k を有限体とするとき, 任意の既約多項式 $f(X) \in k[X]$ は分離的である.

証明 k の標数を p とする. 既約多項式 $f(X) \in k[X]$ に対し, 定理 3.3.13 より, f の被約多項式を g とすると, 負でない整数 e が在って

$$f(X) = g(X^{p^e}) = a_0(X^m)^{p^e} + \cdots + a_{m-1}(X)^{p^e} + a_m \quad (a_i \in k)$$

と表される. α を $f(X)$ の根とすると, $f(X)$ は α の最小多項式であり, 定理 3.1.10 により, $[k(\alpha) : k] = \deg(f)$.

一方 $a \mapsto a^{p^e}$ に依り定められる二つの写像

$$k(\alpha) \longrightarrow k(\alpha), \quad k \longrightarrow k$$

は, 共に $\mathbb{F}_p$ 上の同形写像である. 故に

$$\beta^{p^e} = \alpha, \quad b_i^{p^e} = a_i \quad (i = 0, 1, \cdots m)$$

となる $\beta \in k(\alpha)$, $b_i \in k$ が存在する. このとき $k(\alpha) = k(\beta)$ に注意する.

$$g_1(X) = b_0X^m + \cdots + b_{m-1}X + b_m \ \in k[X]$$

と置くと

$$(g_1(\beta))^{p^e} = g(\beta^{p^e}) = f(\beta) = 0.$$

従って

$$mp^e = \deg(f) = [k(\alpha) : k] = [k(\beta) : k] \leq \deg(g_1) = m$$

となり $e = 0$ を得る. 即ち $f = g$ であり f は分離的である. □

定義 3.3.21 体 k 上の代数拡大が全て分離的なとき, k を **完全体** という.

例 3.3.4 標数 0 の体, 有限体は完全体である.

3.3.4 原始元の存在定理

定理 3.3.22 （原始元の存在定理）有限次分離拡大 K/k は, 単純拡大である. すなわち, 或る $\alpha \in K$ が存在して $K = k(\alpha)$ となる.

証明 k が無限体の場合の証明のみを与える. 有限体の場合の証明に就いては, 例 4.1.4 を参照せよ.

$K = k(\alpha_1, \cdots, \alpha_m)$ と表せる. $m = 2$ の場合を証明すれば, 十分である. $\bar{k}$ を k の代数閉包とし, K の $\bar{k}$ への k 上の埋め込みは, K/k が分離拡大なので, 定理 3.3.11 により, 丁度 $n := [K : k]$ 個存在する. その全体を

$$\sigma_1, \cdots, \sigma_n$$

とする.

$$\sigma_i(\alpha_1) - \sigma_j(\alpha_1), \quad \sigma_i(\alpha_2) - \sigma_j(\alpha_2)$$

は共に 0 となることはない. k は無限体なので

$$c(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)) \neq \sigma_i(\alpha_1) - \sigma_j(\alpha_1) \quad (i \neq j,\ i, j = 1, \cdots, n)$$

を満たす $c \in k$ が存在する.

$$\alpha = c\alpha_1 - \alpha_2$$

とすると

$$\begin{aligned} \sigma_i(\alpha) &= c\sigma_i(\alpha_1) - \sigma_i(\alpha_2) \\ &\neq c\sigma_j(\alpha_1) - \sigma_j(\alpha_2) = \sigma_j(\alpha)\ (i \neq j). \end{aligned}$$

従って

$$n \leq [k(\alpha) : k]_s \leq [k(\alpha) : k] \leq [k(\alpha_1, \alpha_2) : k] = n.$$

よって $k(\alpha_1, \alpha_2) = k(\alpha)$ を得る. □

例 3.3.5 有理数体 $\mathbb{Q}$ に, 1 の三乗根 $\omega = e^{2\pi i/3}$ と $\sqrt[3]{2}$ を添加した体 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ を考える. このとき

$$\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}(\omega + \sqrt[3]{2}) \ni \omega, \sqrt[3]{2}$$

であり, $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\omega + \sqrt[3]{2})$.

例 3.3.6 K/k を n 次分離拡大とする. 定理により $K = k(\alpha)$ と表される. $f(X) \in k[X]$ を α の最小多項式とし,

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n), \quad \alpha = \alpha_1$$

を, K を含む k の代数閉包 $\bar{k}$ における因数分解とする. このとき

$$\sigma_i : K = k(\alpha) \longrightarrow k(\alpha_i), \quad \alpha \longmapsto \alpha_i \ (i = 1, \cdots, n)$$

が K から $\bar{k}$ への k 上の埋め込み全体である. n 次正方行列

$$M = \begin{pmatrix} 1^{\sigma_1} & \alpha^{\sigma_1} & \cdots & (\alpha^{n-1})^{\sigma_1} \\ 1^{\sigma_2} & \alpha^{\sigma_2} & \cdots & (\alpha^{n-1})^{\sigma_2} \\ \vdots & \vdots & \ddots & \vdots \\ 1^{\sigma_n} & \alpha^{\sigma_n} & \cdots & (\alpha^{n-1})^{\sigma_n} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & (\alpha_1)^{n-1} \\ 1 & \alpha_2 & \cdots & (\alpha_2)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & (\alpha_n)^{n-1} \end{pmatrix}, \quad \sigma_j(\alpha_i) = \alpha^{\sigma_j}$$

は正則行列である.

補題 3.3.23 K/k を n 次分離代数拡大とし, K を含む k の代数閉包を $\bar{k}$ とする.

$$\mathrm{Emb}_k(K, \bar{K}) = \{\sigma_1, \cdots, \sigma_n\}$$

とするとき, K/k の任意の基底 $u_1, \cdots, u_n$ に対し, n 次正方行列

$$(u_i^{\sigma_j}), \quad \sigma_j(u_i) = u_i^{\sigma_j}$$

は正則行列である.

証明 $K = k(\alpha)$ $(\exists \alpha \in K)$ と表される. このとき, $(1, \alpha, \cdots, \alpha^{n-1})$ は, K の k 上の基底である. 従って,

$$((u_1, u_2, \cdots, u_n) = (1, \alpha, \cdots, \alpha^{n-1})P$$

を満たす n 次正則行列 P が存在する. このとき,

$$(u_i^{\sigma_j}) = MP$$

が成り立つ. 但し, M は, 前例で与えられた行列である. 従って, 結論を得る. □

3.4 ノルムとトレース

3.4.1 定義と基本的性質

定義 3.4.1 K/k を有限次拡大とし, $\bar{k}$ を, K を含む k の代数閉包とする. K/k の分離次数, 非分離次数を $r=[K:k]_s, s=[K:k]_i$ とし,

$$\mathrm{Emb}_k(K,\bar{k})=\{\sigma_1,\cdots,\sigma_r\}$$

とする. このとき,

$$N_{K/k}(\alpha):=\left(\prod_{i=1}^{r}\sigma_i(\alpha)\right)^s,\quad T_{K/k}(\alpha):=s\left(\sum_{i=1}^{r}\sigma_i(\alpha)\right)$$

を α の **ノルム**, **トレース** という.

定理 3.4.2 K/k を有限次拡大とする. このとき次が成り立つ:

(1) $N_{K/k}:K^\times\longrightarrow k^\times$ は群射である.

(2) $T_{K/k}:K\longrightarrow k$ は k-線形射である.

(3) $L\leq K\leq k$ を体の列とする. このとき,

$$N_{L/k}=N_{K/k}\circ N_{L/K},\quad T_{L/k}=T_{K/k}\circ T_{L/K}.$$

(4) $K=k(\alpha)$ とし,

$$f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$$

を, α の k 上の最小多項式とする. このとき,

$$N_{k(\alpha)/k}(\alpha)=(-1)a_0,\quad T_{k(\alpha)/k}(\alpha)=-a_{n-1}.$$

証明 (1) $[K:k]_i=p^e$ とすると, 系 3.3.19 より, α^{p^e} は k 上分離的である. よって,

$$\beta:=\prod_{i=1}^{r}\sigma_i(\alpha)^{p^e}$$

とおくと β も k 上分離的である. 任意の $\sigma\in\mathrm{Aut}(\bar{k}/k)$ に対し,

$$\{\sigma_1,\cdots,\sigma_r\}=\{\sigma\circ\sigma_1,\cdots,\sigma\circ\sigma_r\}.$$

従って, $\sigma(\beta)=\beta$. 補題 3.3.9 により, $\beta\in k$. $N_{K/k}$ が群射であることは明らかである. (2) も (1) と同様にして示される.
(3) $\mathrm{Emb}_k(K,\bar{k})=\{\sigma_1,\cdots,\sigma_r\}$ とし, σ_i の $\bar{k}\longrightarrow\bar{k}$ への延長を, 同じ文字で表す. また, $\mathrm{Emb}_K(L,\bar{k})=\{\tau_1,\cdots,\tau_t\}$ とする ($[L:K]_s=t$). $\sigma\in\mathrm{End}_k(L,\bar{k})$ に対し, $\sigma|_K=\sigma_i|_K$ $(\exists i)$. 従って, $\sigma_i^{-1}\circ\sigma=\tau_j$ $(\exists j)$ となり,

$$\mathrm{End}_k(L,\bar{k})=\{\sigma_i\circ\tau_j\mid 1\leq i\leq r, 1\leq j\leq t\}.$$

また, $[L:k]_i = [L:K]_i[K:k]_i$ なので, $N_{L/K}(\alpha) \in K$ を考慮すれば,

$$\begin{aligned} N_{L/k}(\alpha) &= \left(\prod_{1\leq i\leq r, 1\leq j\leq t} \sigma_i(\tau_j(\alpha)) \right)^{[L:k]_i} = \left(\prod_{1\leq i\leq r} \sigma_i \left(\prod_{1\leq j\leq t} \tau_j(\alpha) \right)^{[L:K]_i} \right)^{[K:k]_i} \\ &= \left(\prod_{1\leq i\leq r} N_{L/K}(\alpha) \right)^{[K:k]_i} \\ &= N_{K/k}(N_{L/K}(\alpha)). \end{aligned}$$

トレースに就いても同様である.

(4) $[K:k]_s = r, [K:k]_i = p^e$ とし, $\mathrm{Emb}_k(k(\alpha), \bar{k}) = \{\sigma_1, \cdots, \sigma_r\}$ とする. このとき, 定理 3.3.13 により,

$$f(X) = \left(\prod_{i=1}^{r} (X - \sigma_i(\alpha)) \right)^{p^e}$$

である. 従って,

$$N_{k(\alpha)/k}(\alpha) = (-1)a_0, \quad T_{k(\alpha)/k}(\alpha) = -a_{n-1}$$

を得る. □

3.4.2 線形変換としてのノルムとトレース

命題 3.4.3 K/k を有限次拡大とし, $\{w_1, \cdots, w_n\}$ を K/k の基底とする. $\alpha \in K$ に対し,

$$\alpha(w_1, \cdots, w_n) = (w_1, \cdots, w_n)M, \quad M = (m_{ij}) \in \mathrm{M}_n(k)$$

とする.

(1) $\det(M), \mathrm{Tr}(M)$ は, 基底の取り方に依らず定まる. 但し, $\mathrm{Tr}(M) = m_{11} + \cdots + m_{nn}$ は行列 M のトレースである.

(2)

$$N_{K/k}(\alpha) = \det(M), \quad T_{K/k}(\alpha) = \mathrm{Tr}(M)$$

が成り立つ.

証明 (1) は演習問題とする. (2) $\alpha \in K$ に対し, $K/k(\alpha), k(\alpha)/k$ の基底を, それぞれ, $\{u_1, \cdots, u_a\}$, $\{v_1, \cdots, v_b\}$ とする. このとき, $\{u_i v_j \mid 1 \leq i \leq a, 1 \leq j \leq b\}$ は, K/k の基底である.

$$\alpha(v_1, \cdots, v_b) = (v_1, \cdots, v_b)B, \quad B \in \mathrm{M}_b(k)$$

とする.

$$\alpha(u_1v_1, \cdots, u_1v_b, \cdots u_av_b) = (u_1v_1, \cdots, u_1v_b, \cdots u_av_b)M, \quad M \in \mathrm{M}_{ab}(k)$$

とするとき,

$$M = \begin{pmatrix} B & & \\ & \ddots & \\ & & B \end{pmatrix}.$$

但し, 空白部は 0 である. 従って,

$$\det(M) = (\det(B))^a, \quad \mathrm{Tr}(M) = a\mathrm{Tr}(B).$$

一方,

$$N_{K/k}(\alpha) = N_{k(\alpha)/k}(N_{K/k(\alpha)}(\alpha)) = N_{k(\alpha)/k}(\alpha^a) = (N_{k(\alpha)/k}(\alpha))^a.$$

同様にして, $T_{K/k}(\alpha) = aT_{k(\alpha)/k}(\alpha)$. 従って, $K = k(\alpha)$ の場合に帰着された.

α の k 上の最小多項式を

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

とする. $\{1, \alpha, \cdots, \alpha^{n-1}\}$ は $k(\alpha)/k$ の基底である. このとき,

$$\alpha(1, \alpha, \cdots, \alpha^{n-1}) = (1, \alpha, \cdots, \alpha^{n-1})M, \quad M = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & 0 & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

従って,

$$\det(M) = (-1)^n a_0, \quad \mathrm{Tr}(M) = -a_{n-1}$$

が成り立つ. □

3.4.3 分離性とトレース

補題 3.4.4 （E. Artin）$\chi_1, \cdots, \chi_n$ を半群 G から体 K の乗法群 $K^\times$ への相異なる群射とする. このとき, K の元 $a_1, \cdots, a_n$ に対し

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0 \quad \forall g \in G$$

が成立つならば

$$a_1 = \cdots = a_n = 0.$$

証明 $n = 1$ のときは明らか. $\chi_1, \cdots, \chi_n$ の間に自明でない K 上の一次関係式が存在したとし, そのような自明でない関係式の内、最短の関係式を

$$a_1\chi_1 + \cdots + a_m\chi_m = 0 \quad (a_i \neq 0 \ \in K, \ i = 1, \cdots, m)$$

とする. このとき $m \geq 2$ である. $\chi_1 \neq \chi_2$ 故 $\chi_1(g) \neq \chi_2(g)$ となる $g \in G$ が存在する. すべての $h \in G$ に対し

$$a_1\chi_1(gh) + \cdots + a_m\chi_m(gh) = 0,$$

すなわち

$$a_1\chi_1(g)\chi_1 + \cdots + a_m\chi_m(g)\chi_m = 0.$$

この式を $\chi_1(g)$ で割り, 最初の式からひくと

$$(a_2 - a_2\frac{\chi_2(g)}{\chi_1(g)})\chi_2 + \cdots = 0, \quad a_2 - a_2\frac{\chi_2(g)}{\chi_1(g)} \neq 0$$

となる. これは最短の関係式より短い関係式となり, 不合理である. □

補題に於ける G, K を $K^\times, K'$ とすることにより, 次を得る :

系 3.4.5 $\sigma_1, \cdots, \sigma_n$ を体 K から体 K' への相異なる 同形射とするとき, K' の元 $a_1, \cdots, a_n$ に対し

$$a_1\sigma_1(\alpha) + \cdots + a_n\sigma_n(\alpha) = 0 \quad \forall \alpha \in K$$

が成立つならば

$$a_1 = \cdots = a_n = 0.$$

定理 3.4.6 K/k 有限次分離拡大とする. このとき, 次が成り立つ :

(1) $T_{K/k} : K \longrightarrow k$ は零射でない.

(2) 対称双一次形式

$$T : K \times K \longrightarrow k; \quad (x, y) \longmapsto T_{K/k}(xy)$$

は非退化である.

証明 (1) K を含む k の代数閉包を $\bar{k}$ とし, $\mathrm{Emb}_k(K, \bar{k}) = \{\sigma_1, \cdots, \sigma_n\}$ $(n = [K : k])$ とする. すると, 系 3.4.5 により, $\{\sigma_1, \cdots, \sigma_n\}$ は, $\bar{k}$ 上一次独立である. 従って,

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \neq 0 \quad (\exists \alpha \in K).$$

(2) T が対称双一次形式であることはよい. さて, (i) により, $T_{K/k}(\alpha_0) \neq 0$ $(\exists \alpha_0 \in K)$. $\alpha \in K$ に対し, $T(\alpha, \beta) = 0$ $(\forall \beta \in K)$ とする. $\alpha \neq 0$ ならば, $\beta = \alpha_0\alpha^{-1}$ とするとき, $T(\alpha, \beta) = T_{K/k}(\alpha\beta) = T_{K/k}(\alpha_0) \neq 0$ となり不合理である. 従って, $\alpha = 0$ となり, T は非退化である. □

第4章　ガロア理論とその応用

4.1　ガロア理論

K/k を体の拡大とし, $\mathrm{Aut}(K/k)$ を K の, k 上の, 自己同型射全体のなす群とする. K/k がガロア拡大という条件の下で, K/k の中間体と, $\mathrm{Aut}(K/k)$ の部分群の対応を記述する理論をガロア理論という.

4.1.1　ガロア拡大

定義 4.1.1 正規かつ分離的代数拡大 K/k を **ガロア拡大** といい, K の k 上の自己同型射全体のなす群 $\mathrm{Gal}(K/k)$ を, ガロア拡大 K/k の **ガロア群** という.

ガロア拡大 K/k は, その ガロア群 $\mathrm{Gal}(K/k)$ が アーベル群のとき **アーベル拡大**, 巡回群のとき **巡回拡大**, 可解群のとき, **可解拡大** と呼ばれる.

K/k を ガロア拡大とし, その中間体全体のなす集合を $\mathcal{F}(K/k)$ で表し, ガロア群 $\mathrm{Gal}(K/k)$ の部分群全体のなす集合を $\mathcal{G}(K/k)$ で表す. F を K/k の中間体とすると, 補題 3.2.14 により K/F は正規拡大であり, 補題 3.3.12 により K/F は分離拡大である. 従って , K/F は ガロア拡大である. 明らかに $\mathrm{Gal}(K/F)$ は $\mathrm{Gal}(K/k)$ の部分群である.

ガロア群 $\mathrm{Gal}(K/k)$ の部分群 H に対し

$$K^H = \{x \in K \mid \sigma(x) = x\}$$

は K/k の中間体となるが, これを H に対する **不変体** という.

定義 4.1.2 ガロア拡大 K/k の中間体 F に $\mathrm{Gal}(K/F)$ を対応させる写像を

$$g : \mathcal{F}(K/k) \longrightarrow \mathcal{G}(K/k)$$

とする. また, ガロア群 $\mathrm{Gal}(K/k)$ の部分群 H に, その不変体 K^H を対応させる写像を

$$f : \mathcal{G}(K/k) \longrightarrow \mathcal{F}(K/k)$$

とする.

この小節の目的は次の定理を証明することである.

定理 4.1.3 （ガロアの基本定理）K/k を有限次ガロア拡大とし, $G = \mathrm{Gal}(K/k)$ をそのガロア群とする. このとき, 写像 f, g は, 次を満たす:

(1) f, g は全単射であり, 互いに他の逆写像になっている,

(2) $[K : F] = |g(F)|$,

(3) $F \supseteq F' \iff g(F) \subseteq g(F')$,

(4) $g(FF') = g(F) \cap g(F')$,

(5) $g(F \cap F') = \langle g(F), g(F') \rangle$,

(6) F と F' は k 上共役である $\iff g(F)$ と $g(F')$ は G の共役部分群である.

(7) F/k がガロア拡大である $\iff g(F) \triangleleft G$. このとき $\mathrm{Gal}(F/k) \simeq G/g(F) = G/\mathrm{Gal}(K/F)$ が成立つ.

証明　幾つかの補題に分けて証明する.

補題 4.1.4 $K^G = k$.

証明　定義より $k \subseteq K^G$ である. 逆に $\alpha \in K^G$ を任意にとる. $\sigma : k(\alpha) \longrightarrow \bar{K}$ を体 $k(\alpha)$ から K の代数閉包 $\bar{K}$ への k 上の埋め込みとし, それの K への拡張も σ で表す. K/k は正規拡大なので $\sigma \in G$ となる. 仮定により $\alpha^\sigma = \alpha$ であるから, $[k(\alpha) : k]_s = 1$. $k(\alpha)/k$ は分離拡大なので, $[k(\alpha) : k] = [k(\alpha) : k]_s = 1$. 従って $k(\alpha) = k$ となり, $\alpha \in k$ を得る. □

補題 4.1.5　(a) $f \circ g = id$.

(b) g は単射である.

(c) $g(FF') = g(F) \cap g(F')$.

(d) $F \cap F' = f(\langle g(F), g(F') \rangle)$.

(e) $F \subset F' \iff g(F) \supset g(F')$.

証明　(a) F を K/k の中間体とすると, ガロア拡大 K/F に補題 4.1.4 を適用すると

$$f(g(F)) = K^{\mathrm{Gal}(K/F)} = F.$$

(b) は (a) より直ちに得られる.
(c) $\sigma \in g(FF')$ とすると, σ は F の元 F' の元を共に不変にする. すなわち $\sigma \in g(F), \sigma \in g(F')$. 従って $\sigma \in g(F) \cap g(F')$. 逆も同様である.
(d) $x \in$ 左辺とする. x は $g(F) = \mathrm{Gal}(K/F), g(F') = \mathrm{Gal}(K/F')$ の元で不変である. 従ってそれらで生成される群 $\langle g(F), g(F') \rangle$ の元で不変である. 故に $x \in$ 右辺. 逆に, $x \in$ 右辺とすると, x は $g(F), g(F')$ の元で不変であるから, 補題 4.1.4 を $k = F, F'$ として適用すると, F, F' に含まれることがわかる.
(e) ($\Longrightarrow$) は明らかである. ($\Longleftarrow$) $x \in F$ ならば x は $g(F)$ 不変である. 従って $g(F')$ 不変となり $x \in F'$ を得る. □

補題 4.1.6 K を体とし, G を $\mathrm{Aut}(K)$ の位数 n の有限部分群とする. このとき K/K^G は, n 次ガロア拡大で, そのガロア群は G となる.

証明 （E. Artin）$\alpha \in K$ を任意にとる. G の部分集合 $\sigma_1, \cdots, \sigma_r$ を

$$\sigma_1(\alpha), \cdots, \sigma_r(\alpha)$$

が互に異なるような極大なものとする. 任意の $\tau \in G$ に対し $\tau\sigma_i(\alpha)$ は, ある $\sigma_j(\alpha)$ に一致する. さもないと極大性に反する. しかも τ は単射なので

$$\{\tau\sigma_1(\alpha), \cdots, \tau\sigma_r(\alpha)\} = \{\sigma_1(\alpha) \cdots, \sigma_r(\alpha)\}.$$

よって,

$$f(X) = \prod_{i=1}^{r}(X - \sigma_i(\alpha))$$

とすると

$$f^\tau = f, \quad \forall \tau \in G.$$

従って, $f(X)$ の係数は $k = K^G$ に含まれる. 作り方より, f は分離多項式なので, α は k 上分離的である. α は任意であったから, K/k は分離拡大である. α の最小多項式は, f の因子であるので, その次数は n 以下である. 更に K/k の拡大次数も n 以下となる. もし $[K : k] > n$ ならば, $[F : k] = m > n$ となる中間体が存在する. 有限次分離拡大には原始元, 即ち $F = k(\alpha)$ となる α が存在する. このとき α の最小多項式の次数は m となり, 上で述べたことと矛盾する. よって, $[K : k] \leq n$. さて $K = k(\alpha)$ とすると $\sigma(\alpha)$ $(\sigma \in G)$ は互に異なるので, $[K : k] \geq n$. 従って $[K : k] = n$. また K は α の最小多項式

$$f(X) = \prod_{\sigma \in G}(X - \sigma(\alpha))$$

の分解体である. 従って 定理 3.2.13 により K/k は正規拡大であることを知る. □

補題 4.1.7 g は全単射である.

証明 g が単射であることは既に知っている. H を $\mathrm{Gal}(K/k)$ の任意の部分群とする. $F = K^H$ とすれば, 前補題により K/F は ガロア拡大で, その ガロア群は $g(F) = H$ となる. 従って g は全射である. □

補題 4.1.8 $F \in \mathcal{F}(K/k), H \in \mathcal{G}(K/k), \sigma \in \mathrm{Gal}(K/k)$ に対し, $\sigma(F) = F^\sigma, \sigma H \sigma^{-1} = H^\sigma$ と表すこととする.

(a) $g(F^\sigma) = g(F)^\sigma, \quad F^\sigma = f(g(F)^\sigma), \quad \forall \sigma \in G$.

(b) F/k が ガロア拡大 $\Longleftrightarrow \mathrm{Gal}(K/F) \lhd G$.

(c) F/k が ガロア拡大ならば, 制限写像

$$G \longrightarrow \mathrm{Gal}(F/k), \quad \sigma \mapsto \sigma|_F$$

は群全射で, その核は $\mathrm{Gal}(K/F)$ である. 従って

$$\mathrm{Gal}(F/k) \simeq G/\mathrm{Gal}(K/F).$$

証明　(a) $\tau \in g(F^\sigma) = \mathrm{Gal}(K/F^\sigma)$ とすると, 任意の $x \in F$ に対し

$$\tau(\sigma(x)) = \sigma(x), \quad i.e., \quad (\sigma^{-1}\tau\sigma)(x) = x.$$

従って $\sigma^{-1}\tau\sigma \in g(F)$ となり, $\tau \in \sigma g(F)\sigma^{-1} = g(F)^\sigma$. よって, $g(F^\sigma) \subseteq g(F)^\sigma$ を得る. 逆の包含関係も同様にして得られ, $g(F^\sigma) = g(F)^\sigma$ が成り立つ. この式に f を作用させ, $f \circ g = id$ を用いると $F^\sigma = f(g(F)^\sigma)$ を得る.
(b) F/k は分離拡大であり (補題 3.3.12), これがガロア拡大である為には

$$F^\sigma = F \quad \forall \sigma \in G \tag{4.1}$$

となることである. 何故ならば, F/k が正規拡大ということは, 任意の k 上の埋め込み $\sigma : F \rangle \bar{F}$ に対し $\sigma(F) = F$ となることである (補題 3.2.12). σ を K まで拡張したものを, 改めて σ と書けば K/k がガロア拡大なので $\sigma \in G$ となるからである. さて (a) より, (4.1) は

$$g(F) = g(F)^\sigma \quad \forall \sigma \in G,$$

すなわち, $g(F)$ が G の正規部分群となることである.
(c) F/k を ガロア拡大とするとき, 制限写像

$$G \longrightarrow \mathrm{Gal}(F/k), \quad \sigma \mapsto \sigma|_F$$

は群射であり, その核は $\mathrm{Gal}(K/F)$ である. また, 任意の $\tau \in \mathrm{Gal}(F/k)$ に対し, K から $\bar{K}$ への τ 上の埋め込みを τ' とすると $\tau' \in G$ であり, その F への制限は τ である. よって制限写像は全射であり, 群の同型定理により

$$G/\mathrm{Gal}(F) \simeq \mathrm{Gal}(F/k)$$

を得る. □

以上により, 基本定理の証明は完結した.

この様にして有限次ガロア拡大 K/k の中間体と，ガロア群 $\mathrm{Gal}(K/k)$ の部分群との完璧な対応が得られたのである. これは数学の中で最も ‘‘ 美しい ’’ 理論の一つであり, このガロア理論の発見の後，様々な拡張や類似の理論の構築が試みられた.

4.1.2　基本定理の補足

補題-定義 4.1.9　E/k を有限次分離拡大とし, K/k を E を含む最小の正規拡大とする. このとき K/k は有限次ガロア拡大である. K は, E を含む, k の最小のガロア拡大で E/k の **ガロア閉包** と呼ばれる.

証明　$[E : k] = n$ とし $\sigma_1, \cdots, \sigma_n$ を E の代数閉包 $\bar{E}$ への k 上の埋め込み全体とする. E を含む最小の正規拡大 K/k は

$$K = \sigma_1(E) \cdots \sigma_n(E)$$

で与えられる (補題 3.2.15). $\sigma_i(E)/k$ は有限次分離拡大であるので, 補題 3.3.12 により, K/k は分離拡大, 従って有限次ガロア拡大であることがわかる. □

補題 4.1.10 K/k を有限次ガロア拡大, F/k を任意の拡大とし, K, F は共にある体に含まれているとする. このとき次が成立つ.

(1) KF/F, $K/(K\cap F)$ はガロア拡大である.

(2) 制限写像

$$\mathrm{Gal}(KF/F) \longrightarrow \mathrm{Gal}(K/k), \quad \sigma \longmapsto \sigma|_K$$

は単射であり, その像は $\mathrm{Gal}(K/(K\cap F))$ に一致する.

(3) $[KF:K]|[K:k]$.

証明 (1) KF/F については, 補題 3.3.12 と補題 3.2.14 により, $K/(K\cap F)$ については, 定理 4.1.3 により, ガロア拡大であることを知る.
(2) 制限写像 $\mathrm{Gal}(KF/F)\rangle\mathrm{Gal}(K/k)$ が単射であることは明らか. その像を H とすると, $K^H \supset K\cap F$ が成立つ. 逆に $\alpha \in K^H$ ならば $\alpha \in K\cap F$ が成立ち, $K^H = K\cap F$ である. K/k が有限次ガロア拡大ならば, 補題 4.1.6 により, $K/K^H = K/K\cap F$ はガロア拡大であり, その ガロア群 $\mathrm{Gal}(K/K\cap F)$ は H である.
(3) は (2) より直ちにわかる. □

例 4.1.1 K/k がガロアでないと上の補題の (3) は, 一般には, 成立しない. 例えば ω を 1 の虚数立方根とし

$$K = \mathbb{Q}(\sqrt[3]{2}),\ F = \mathbb{Q}(\omega\sqrt[3]{2})$$

とする. このとき

$$KF = \mathbb{Q}(\sqrt[3]{2}, \omega) = F(\omega)$$

は $X^3 - 2$ $\mathbb{Q}$ 上の分解体で

$$[KF:F] = [F(\omega):F] = 2 \not| [K:\mathbb{Q}] = 3.$$

補題 4.1.11 $K_1/k, K_2/k$ を ガロア拡大とし, K_1, K_2 は共にある体の部分体とする. このとき合成体 K_1K_2/k はガロア拡大で, 群準同型写像

$$\phi : \mathrm{Gal}(K_1K_2/k) \longrightarrow \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k), \quad \sigma \mapsto (\sigma|K_1, \sigma|K_2)$$

は単射であり, $K_1\cap K_2 = k$ ならば, これは同型写像である.

証明 補題 3.3.12 と補題 3.2.14 により, K_1K_2/k がガロア拡大であることがわかる. 写像 ϕ が群単射であることは明らかである.
$K_1\cap K_2 = k$ とすると, 補題 4.1.10 により, 制限写像

$$\mathrm{Gal}(K_1K_2/K_2) \longrightarrow \mathrm{Gal}(K_1/k), \quad \sigma \mapsto \sigma|_{K_1}$$

は同型射であることを知る. すなわち, 任意の $\sigma_1 \in \mathrm{Gal}(K_1/k)$ に対し, $\sigma \in \mathrm{Gal}(K_1K_2/K_2)$ で, その K_1 への制限が σ_1 となるものが存在する. このとき $\sigma \in \mathrm{Gal}(K_1K_2/k)$ である. 従って

$$\phi(\mathrm{Gal}(K_1K_2/k)) \supseteq \mathrm{Gal}(K_1/k) \times \{1\}.$$

同様にして

$$\phi(\mathrm{Gal}(K_1K_2/k)) \supseteq \{1\} \times \mathrm{Gal}(K_2/k).$$

よって ϕ は全射であることがわかる. □

4.1.3　代数学の基本定理の証明

ガロア理論を用いて, 代数学の基本定理 3.1.17 の純代数的証明を与える.
以下の事実を用いて証明する.

(1) 実係数奇数次代数方程式は必ず実根を持つ.

(2) 複素数係数二次代数方程式は必ず複素数根を持つ.

(3) Sylow 部分群の存在定理.

(4) p-群は, 指数 p の部分群を持つ.

$k/\mathbb{C}$ を任意の代数拡大とし, K を $k/\mathbb{R}$ のガロア閉包, $G = \mathrm{Gal}(K/\mathbb{R})$ とする. H を G の 2-Sylow 部分群とし $F = K^H$ とすると, $[F : \mathbb{R}]$ は奇数である. $F/\mathbb{R}$ は有限次分離拡大なので, 定理 3.3.22 により, 原始元が存在する. すなわち $F = \mathbb{R}(\alpha)$ となる α が存在する. α の最小多項式 $f(X)$ の次数は, $[F : \mathbb{R}]$ に等しく, 奇数である. 一方, 実係数奇数次代数方程式は必ず実根を持つので, f は一次式となり, $F = \mathbb{R}$. 従って $G = H$ となり, G は 2-群である. $k \neq \mathbb{C}$ とすると, $\mathrm{Gal}(K/\mathbb{C})$ は自明ではない 2-群である. 従って, $\mathrm{Gal}(K/\mathbb{C})$ は指数 2 の部分群 G' を持つ. G' に対する不変部分体 $K' = K^{G'}$ は $\mathbb{C}$ の二次拡大体である. 複素数係数二次多項式は, $\mathbb{C}[X]$ において一次式の積に分解する. 従って複素数体 $\mathbb{C}$ は二次拡大体を持たない. これは不合理であり, $k = \mathbb{C}$ を得る. すなわち $\mathbb{C}$ の真の代数拡大は存在せず, 複素数体は代数閉体である. □

4.1.4　巡回拡大

補題 4.1.12　（ Hilbert の定理 90）K/k を 有限次巡回拡大とし, $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ とする. $\beta \in K$ に対し, 次は同値である.

(1) $\mathrm{N}_{K/k}(\beta) = 1$.

(2) $\beta = \alpha/\sigma(\alpha)$ となる $\alpha(\neq 0) \in K$ が存在する.

証明　(2) $\Longrightarrow$ (1) は明らかである.
(1) $\Longrightarrow$ (2) $[K : k] = n$ とすると, $1, \sigma, \cdots, \sigma^{n-1}$ は相異なる. 従って, 系 3.4.5 により,

$$1 + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \cdots + (\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta))\sigma^{n-1}$$

は K 上恆等的には 0 ではない. すなわち, ある $\theta \in K$ が存在して

$$\alpha := \theta + \beta\sigma(\theta) + (\beta\sigma(\beta))\sigma^2(\theta) + \cdots + (\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta))\sigma^{n-1}(\theta) \neq 0.$$

両辺に σ を施し, β をかけ, $\mathrm{N}_{K/k}(\beta) = 1$ に注意すると $\beta\sigma(\alpha) = \alpha$ を得る. □

定理 4.1.13 K/k を体の拡大とし, $(n, \mathrm{char}(k)) = 1$ とする. 1 の原始 n 乗根が k に含まれるとき, 次は同値である.

(1) K/k は巡回拡大で, $[K : k] \,|\, n$.

(2) $K = k(\sqrt[n]{a}) \quad (a \in k^\times)$.

証明 (1) $\Longrightarrow$ (2) $d := [K : k]$ とし, ζ を 1 の原始 d 乗根とする. $d|n$ なので, $\zeta \in k$ である. 巡回群 $\mathrm{Gal}(K/k)$ の生成元を σ とすると, $N_{K/k}(\zeta^{-1}) = (\zeta^d)^{-1} = 1$ なので, Hilbert の定理 90 により, $\sigma(\alpha) = \zeta\alpha$ を満たす $\alpha\ (\neq 0) \in K$ が存在する. このとき

$$\sigma^i(\alpha) = \zeta^i\alpha \quad (i = 1, \cdots, d)$$

は互に異なる. 従って $[k(\alpha) : k] \geq d$ である. 一方 $[K : k] = d$ より $K = k(\alpha)$ となる. また

$$\sigma(\alpha^d) = \sigma(\alpha)^d = (\zeta\alpha)^d = \alpha^d$$

となり, $\alpha^d \in k$. 従って $(\alpha^d)^{n/d} = a$ とすれば, $\alpha = \sqrt[n]{a}$ である.
(2) $\Longrightarrow$ (1) ζ を 1 の原始 n 乗根とし, α を $X^n - a = 0$ の解とする. このとき, $\zeta^i\alpha$ も解である. 従って $X^n - a = 0$ の全ての解は $k(\alpha)$ に含まれる. よって $k(\alpha)$ は $X^n - a$ の分解体である. また, これらの解は互に異なるので, $k(\alpha)/k$ は ガロア拡大である. 任意の $\sigma \in \mathrm{Gal}(k(\alpha)/k)$ に対し

$$\sigma(\alpha) = \omega_\sigma\alpha$$

と書ける. ただし ω_σ は 1 の n 乗根であるが, 原始 n 乗根とは限らない. σ に ω_σ を対応させる写像

$$\phi : \mathrm{Gal}(k(\alpha)/k) \longrightarrow \langle\zeta\rangle$$

は群単射である. 巡回群の部分群は巡回群なので $\mathrm{Gal}(k(\alpha)/k)$ は巡回群である. その位数を d とすると $d|n$ である. また σ を $\mathrm{Gal}(k(\alpha)/k)$ の生成元とすれば, ω_σ は 1 の原始 d 乗根である. □

4.1.5 有限体

正標数 p の素体 $\mathbb{F}_p$ の代数閉包 $\bar{\mathbb{F}}_p$ を一つ固定し, $\bar{\mathbb{F}}_p$ の部分体のみを考える. $q = p^n$ とし, 分離多項式

$$X^q - X \tag{4.2}$$

の根全体 $\mathbb{F}_q$ を $\bar{\mathbb{F}}_p$ の中で考える. すると $\mathbb{F}_q$ は体をなし, 多項式 (4.2) の $\mathbb{F}_p$ 上の最小分解体である. 従って, 定理 3.2.13 と定理 3.3.17 により, $\mathbb{F}_q/\mathbb{F}_p$ は n 次ガロア拡大である.

例 4.1.2 $X^4 - X = X(X^3 - 1) \in \mathbb{F}_2[X]$ の $\bar{F}_2$ に於ける因数分解を

$$X(X - 1)(X - \omega)(X - \omega^2)$$

とする.

$$\phi : \mathbb{F}_2[X] \longrightarrow \mathbb{F}_2(\omega), \quad g(X) \longmapsto g(\omega)$$

は環全射で, その核は (X^2+X+1). 従って

$$\mathbb{F}_2[X]/(X^2+X+1) \simeq \mathbb{F}_2(\omega) = \mathbb{F}_4.$$

例 4.1.3 $f(X) = X^2+1 \in \mathbb{F}_3[X]$ は既約多項式である. $f(X)=0$ の解の一つを $\alpha \in \bar{F}_3$ とするとき

$$\phi : \mathbb{F}_3[X] \longrightarrow \mathbb{F}_3[\alpha] = \mathbb{F}_3(\alpha),$$

は環全射であり,

$$\mathbb{F}_3[X]/(X^2+1) \simeq \mathbb{F}_3[\alpha] = \mathbb{F}_9.$$

K を標数 p の任意の有限体とし $[K:\mathbb{F}_p] = n$ とすれば $|K| = p^n = q$ である. 定理 1.3.23 より, 体の乗法群の有限部分群は巡回群なので, $K^\times$ は位数 $q-1$ の巡回群である. $K^\times = \langle\theta\rangle$ とすると

$$K = \{0, 1, \theta, \cdots, \theta^{q-2}\}$$

と表される. 従って K の全ての元は, 分離多項式 $X^q - X$ の根である. よって, $K = \mathbb{F}_q$ を得る.

従って次の定理を得た.

定理 4.1.14 $q = p^n$ 個の元からなる有限体は $X^q - X$ の最小分解体である.

例 4.1.4 K/k を有限体の有限次拡大とする. $K^\times = \langle\theta\rangle$ とすれば,

$$K = k(\theta).$$

すなわち, K/k は単純拡大である.

定理 4.1.15 任意の自然数 f に対し, $\mathbb{F}_{q^f}/\mathbb{F}_q$ は f 次巡回拡大で, そのガロア群は

$$\sigma = \sigma_F : \mathbb{F}_{q^f} \longrightarrow \mathbb{F}_{q^f}, \quad \alpha = \alpha^q$$

で生成される.

証明 $\mathbb{F}_{q^f}/\mathbb{F}_p$ はガロア拡大なので, $\mathbb{F}_{q^f}/\mathbb{F}_q$ もガロア拡大である. また

$$\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) \supseteq \{1, \sigma, \cdots, \sigma^{f-1}\}$$

は容易に分かり, 位数を比べこれらが等しいことを得る. 故に $\mathbb{F}_{q^f}/\mathbb{F}_q$ は f 次巡回拡大である. □

4.1.6　円分体

代数閉体 Ω として複素数体 $\mathbb{C}$ を採り, 多項式 $X^n - 1$ の, $\mathbb{Q}$ 上の最小分解体 $\mathbb{Q}(\zeta_n)$ を n 次の**円分体** という. 自然数 n に対し, $\varphi(n)$ 次の多項式

$$\Phi_n(X) = \prod_{\zeta:\text{原始 } n \text{ 乗根}} (X - \zeta)$$

を **円（の n 等）分多項式** という.

定理 4.1.16 円分多項式 $\Phi_n(X)$ は, 有理整数係数多項式であり, 1 の原始 n 乗根 ζ_n の $\mathbb{Q}$ 上の最小多項式である. また $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ のガロア群は $(\mathbb{Z}/n\mathbb{Z})^\times$ に同形である.

証明 ζ を 1 の原始 n 乗根とし, $f(X) \in \mathbb{Q}[X]$ を ζ の最小多項式とする. すると f は $X^n - 1$ を割切るので

$$X^n - 1 = f(X)g(X), \quad \exists g(X) \in \mathbb{Q}[X].$$

f, g の最高次係数は, 共に 1 であるので, 補題 2.6.10 により $f(X), g(X) \in \mathbb{Z}[X]$.

$\Phi_n(X) = f(X)$ が成り立つことを, いくつかのステップに分けて示す.

(Step 1) η が $f(X) = 0$ の根ならば, n を割らない素数 p に対し, η^p も $f(X) = 0$ の根である.

もし η^p が $f(X)$ の根でなければ, $g(X)$ の根である. 従って η 自身は $g(X^p)$ の根である. f は η の最小多項式でもあるので $q(X^p)$ を割切る. 即ち

$$g(X^p) = f(X)h(X), \quad \exists h(X) \in \mathbb{Q}[X].$$

上と同じ理由により $h(X) \in \mathbf{Z}[X]$. 一方, 整数 a に対し, $a^p \equiv a \pmod{p}$ が成り立つので,

$$g(X^p) \equiv g(X)^p \equiv f(X)h(X) \pmod{p} \tag{4.3}$$

が成り立つ. f, g の係数を $\mathbb{F}_p = \mathbf{Z}/p\mathbf{Z}$ の元と見なしたものを $\bar{f}(X), \bar{g}(X) \in \mathbb{F}_p[X]$ と表すことにすると, (4.3) より, $\bar{f}$ と $\bar{g}$ とは互に素ではない. 従って, $\mathbb{F}_p[X]$ において $X^n - 1 = \bar{f}(X)\bar{g}(X)$ なので, $\bar{\mathbb{F}}_p$ において, $X^n - 1$ は重根を持つ. しかし, $(p, n) = 1$ より, $X^n - 1 \in \mathbb{F}_p[X]$ は分離多項式であるので, これはあり得ない. 従って η^p は $f(X) = 0$ の根である.

(Step 2) η を任意の原始 n 乗根とすると, η は $f(X) = 0$ の根であることを示す.

$\eta = \zeta^m, (n, m) = 1$ と表される. $m = p_1 \cdots p_t$ を m の素因数分解とすれば, ζ^{p_1} は (Step 1) により, $f = 0$ の根である. 再び (Step 1) により, $\zeta^{p_1 p_2}$ も $f = 0$ の根である. 以下同様にして η も $f = 0$ の根である.

(Step 3) $f(X) = \Phi_n(X)$ であることを示そう.

$f = 0$ の根が全て 1 の原始 n 乗根であることを示せば, (Step 2) より (Step 3) を得る. $f(\eta) = 0$ とすると, $f(X)$ は η の最小多項式である. もし η が 1 の原始 n 乗根でなければ

$$\eta = \zeta^m, \quad d = (n, m) > 1$$

と表され

$$(\eta)^{\frac{n}{d}} - 1 = \zeta^{m\frac{n}{d}} - 1 = 0.$$

すると f は $X^{\frac{n}{d}} - 1$ を割り, $(\zeta)^{\frac{n}{d}} = 1$ となり矛盾する. よって, $f(X)$ の根は, 全て, 1 の原始 n 乗根である.

以上により, $\Phi_n(X) = f(X)$ が示された. また, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$ なので, 命題 **??** より, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. □

例 4.1.5 円分体 $\mathbb{Q}[\zeta_n]$ は円分多項式 $\Phi_n(X)$ の分解体である.

例 4.1.6 p を奇素数とし,

$$\zeta := \zeta_p = e^{\frac{2\pi}{p}}$$

とする. このとき

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1 = (X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1}).$$

$\Phi_p(X)$ に 1 を代入して

$$p = \Phi_p(1) = \prod_{i=1}^{p-1}(1-\zeta^i) = \prod_{i=1}^{\frac{p-1}{2}}(1-\zeta^i)(1-\zeta^{p-i})$$

を得る.

$$(1-\zeta^i)(1-\zeta^{p-i}) = (1-\zeta^i)(1-\zeta^{-i}) = -\zeta^{-i}(1-\zeta^i)^2$$

なので

$$p = (-1)^{\frac{p-1}{2}}\zeta^Q \prod_{i=1}^{\frac{p-1}{2}}(1-\zeta^i)^2, \quad Q = 1+2+\cdots+\frac{p-1}{2} = \frac{p^2-1}{4}.$$

従って, p は奇数なので, Q は偶数であり, $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}(\zeta_p)$.

ガロア群 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p-1$ の巡回群であり, 位数 2 の部分群に対応する部分体は

$$\mathbb{Q}(2\cos(2\pi/p)) = \mathbb{R} \cap \mathbb{Q}(\zeta), \quad \zeta + \zeta^{p-1} = 2\cos(2\pi/p).$$

$\mathbb{Q}(2\cos(2\pi/p))$ を, 円分体 $\mathbb{Q}(\zeta)$ の **最大実部分体** という.

また, $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ は $\mathbb{Q}(\zeta_p)$ に含まれる, 唯一の二次体である.

系 4.1.17 m, n を互いに素な正整数とするとき, 次が成立つ.

(1) $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

(2) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

証明 $(m,n) = 1$ 故 $rm + sn = 1$ を満たす整数 r, s が存在する. このとき

$$\zeta_{mn} = (\zeta_{mn})^{rm}(\zeta_{rm})^{sn}.$$

$(\zeta_{mn})^m, (\zeta_{mn})^n$ は, それぞれ 1 の原始 n, m 乗根である. 従って, $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ を得る. また,

$$\begin{aligned}[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] &= [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] \\ &= \varphi(mn) = \varphi(m)\varphi(n)\end{aligned}$$

が成立ち, $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] = \varphi(m)$ を得る. 一方, 補題 4.1.10 により

$$\begin{aligned}\varphi(m) = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] &= [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)] \\ &\leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m).\end{aligned}$$

よって $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$ でなければならない. □

アーベル拡大 $\mathbb{Q}(\zeta_n)$ の部分体はアーベル拡大であるが, その逆も成り立つ.

定理 4.1.18 （Kronecker-Weber） $\mathbb{Q}$ 上の任意のアーベル拡大はある円分体 $\mathbb{Q}(\zeta_n)$ の部分体である.

この定理の証明は程度を超えるので省略する. 有限次代数体上のアーベル拡大の理論を **類体論** という.

4.2 代数方程式の冪根による解法

この節で取り扱う体は, 特に断らない限り, すべて複素数体の部分体とする. 従って, 任意の代数拡大は分離代数拡大である.

4.2.1 冪根拡大と代数的可解性

代数方程式が, 代数的に解けるということをはっきりさせよう. 体の拡大 K/k は, 次のような体の列が存在するとき, **冪根拡大** と呼ばれる：

$$k=K_0\subset K_1\subset\cdots\subset K_r=K;\quad K_i=K_{i-1}(\sqrt[n_i]{\alpha_i}),\quad \alpha_i\in K_{i-1},\ 2\le n_i\in\mathbb{Z}.$$

k 係数多項式, $f(X)$ の（k 上の）最小分解体を K_f とする. $K_f\subset K$ となる冪根拡大 K/k が存在するとき, 代数方程式 $f(X)=0$ は k 上 **代数的に解ける** という.

二次方程式, 三次方程式, 四次方程式は代数的に解けることを確かめよう.

a,b を複素数とし, $k=\mathbb{Q}(a,b)$ とする. 二次式 $f(X)=X^2+aX+b$ の分解体は

$$K_f=k(\sqrt{D}),\quad D=a^2-4b\in k.$$

従って $X^2+aX+b=0$ は, k 上代数的に解ける.

2. 三次方程式の Cardano による解法 k を体とし, k 係数既約三次多項式

$$X^3+a_1X^2+a_2X+a_3\quad\in k[X]$$

を考える.

$$X=Y-\frac{a_1}{3}$$

を代入し, Y を改めて X と書く:

$$f(X):=X^3+pX+q,\quad p=-\frac{a_1^2}{3}+a_2,\ q=\frac{2a_1^3}{27}-\frac{a_1a_2}{3}+a_3. \tag{4.4}$$

ここで,

$$X=u+v$$

を代入すると

$$f(u+v) = u^3 + v^3 + (3uv+p)(u+v) + q.$$

従って,

$$3uv + p = 0,\ u^3 + v^3 + q = 0 \tag{4.5}$$

ならば $f(u+v) = 0$.

さて, 式 (4.5) を仮定すると, u^3, v^3 は, 二次方程式

$$\phi(t) := t^2 + qt - \frac{p^3}{27} = 0 \tag{4.6}$$

の根である. $\phi(t)$ の判別式を

$$D := q^2 + \frac{4p^3}{27}$$

とすれば

$$u^3 = \frac{-q+\sqrt{D}}{2}, \quad v^3 = \frac{-q-\sqrt{D}}{2}$$

となる. そこで,

$$U = \sqrt[3]{\frac{-q+\sqrt{D}}{2}}, \quad V = \sqrt[3]{\frac{-q-\sqrt{D}}{2}}$$

を, $3UV = -p$ を満たすようにとり, $\omega = e^{2\pi i/3}$ とすれば,

$$3(\omega U)(\omega^2 V) = p, \quad 3(\omega^2 U)(\omega V) = p.$$

このとき

$$\alpha_1 = U + V, \quad \alpha_2 = \omega U + \omega^2 V, \quad \alpha_3 = \omega^2 U - \omega V$$

が, 方程式 (4.4) の三個の解である. 二次方程式 (4.6) を (4.4) の**分解方程式** という.

$$K_1 = k(\sqrt{-3}), \quad K_2 = K_1(\sqrt{D}), \quad K_3 = K_2\left(\sqrt[3]{\frac{-q+\sqrt{D}}{2}}\right)$$

とすれば, $V = -p/(3U) \in K_3$ であり,

$$k \subset K_1 \subset K_2 \subset K_3, \quad K_f \subset K_3$$

を得る. 従って $f(X) = 0$ は代数的に解ける.

例 4.2.1 方程式 $X^3 - 3x + 1 = 0$ を解いてみよう. $X = u + v$ を代入し,

$$u^3 + v^3 + (3uv - 3)(u+v) + 1 = 0.$$

u^3, v^3 は $t^2 + t + 1 = 0$ の二根であり,

$$u^3 = \frac{-1+\sqrt{-3}}{2} = \omega = e^{\frac{2\pi i}{3}}, \quad v^3 = \omega^2.$$

$$U = \zeta := e^{\frac{2\pi i}{9}}, \quad V = \omega^2\zeta^2 = \zeta^8$$

とすれば, $3UV = 3\omega^3 = 3$ を満たす. 従って, 求める解は,

$$\begin{array}{lcccl} U+V & = & \zeta+\zeta^8 & = & 2\cos\frac{2\pi}{9}, \\ \omega U+\omega^2 V & = & \zeta^4+\zeta^5 & = & 2\cos\frac{8\pi}{9}, \\ \omega^2 U+\omega V & = & \zeta^7+\zeta^2 & = & 2\cos\frac{4\pi}{9}. \end{array}$$

3. 四次方程式の Ferrari による解法

既約四次方程式

$$f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 = 0 \quad (a_i \in k)$$

の解法を考えよう. 三次の場合と同様に, X を $X - a_1/4$ とすると, 3 次の項が消えて,

$$f(X) = X^4 + pX^2 + qX + r = 0$$

を得る. $q = 0$ の場合, $f(X) = 0$ の解法は容易であるので, $q \neq 0$ として議論を進める. この方程式の解を $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ とし,

$$\beta_1 = \frac{1}{2}(\alpha_1\alpha_3 + \alpha_2\alpha_4),\ \beta_2 = \frac{1}{2}(\alpha_1\alpha_2 + \alpha_3\alpha_4),\ \beta_3 = \frac{1}{2}(\alpha_1\alpha_4 + \alpha_2\alpha_3)$$

と置く.

$$A = \beta_1 + \beta_2 + \beta_3, \quad B = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3, \quad C = \beta_1\beta_2\beta_3$$

とすると, A, B, C は, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ の対称式であり, p, q, r の多項式として表される. 実際, $\beta_1, \beta_2, \beta_3$ を根として持つ多項式は

$$g(T) = T^3 - \frac{p}{2}T^2 - rT + \frac{4pr - q^2}{8}$$

と表される. $g(T)$ を分解方程式という. t を $g(T) = 0$ の解とし, $X^4 = -pX^2 - qX - r$ の両辺に, $2tX^2 + t^2$ を加えると

$$(X^2 + t)^2 = (2t - p)X^2 - qX + (t^2 - r)$$

を得る. $t = p/2$ ならば $q = 0$ となることに注意する. 右辺の二次式の判別式は, t の取り方により, 0 に等しい. 従って,

$$X^2 + t^2 = \pm\sqrt{2t - p}\left(X - \frac{q}{2(2t - p)}\right).$$

この方程式を解いて, $f(X) = 0$ の四個の解を得る. $g(T) = 0$ は代数的に解け, 二次方程式も代数的に解けるので, $f(X) = 0$ は, k 上代数的に解ける.

例 4.2.2 四次方程式 $X^4 + 4X - 1 = 0$ の分解三次方程式は, $g(T) = T^3 + T - 2 = 0$ である. $g(1) = 0$ なので,

$$(X^2 + 1)^2 = 2X^2 - 4X + 2 = 2(X + 1)^2$$

を得る. 従って, $X^2 + 1 = \pm\sqrt{2}(X + 1)$, 即ち, $X^2 \pm \sqrt{2}(X + 1) = 0$ を解いて, 四個の解

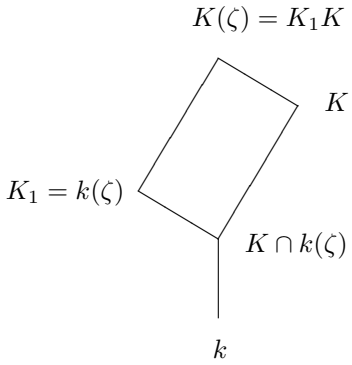
$$X = \frac{-\sqrt{2} \pm \sqrt{2 - 4\sqrt{2}}}{2}, \quad \frac{\sqrt{2} \pm \sqrt{2 + 4\sqrt{2}}}{2}$$

を得る.

4.2.2　代数方程式の代数的可解性と可解拡大

定理 4.2.1 k を体とし, 一次以上の多項式 $f(X) \in k[X]$ は重根を持たないとする. $f(X)$ の k 上の最小分解体を K とするとき, 代数方程式 $f(X) = 0$ が k 上代数的に解ける為の必要十分条件は K/k が可解拡大となることである.

証明　（十分性）K/k を可解拡大とし, $[K : k] = n$ とする. ζ を 1 の原始 n 乗根とし $K_1 = k(\zeta)$ とすると 定理 4.1.16 により, K_1/k はアーベル拡大である. このとき次の図を得る：

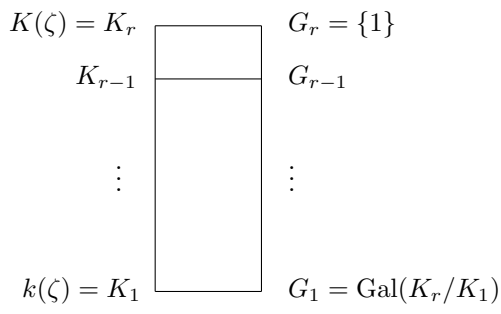


補題 4.1.11 により, $K(\zeta)/k$ はガロア拡大である. 従って, 補題 4.1.10 により, $K(\zeta)/K_1$ もガロア拡大であり, $\mathrm{Gal}(K(\zeta)/K_1) \simeq \mathrm{Gal}(K/K_1 \cap K)$ が成り立つ. この群は可解群 $\mathrm{Gal}(K/k)$ の部分群なので, 定理 1.7.14 により, 可解群でありその位数は n の約数である. 可解群の定義と有限アーベル群の構造定理 1.9.17 を組合せると, 次の様な部分群の列を得る.

$$\{1\} = G_r \subset G_{r-1} \subset \cdots \subset G_1 = \mathrm{Gal}(K(\zeta)/K_1),$$

$$G_i \triangleleft G_{i-1}, \quad G_{i-1}/G_i : \text{位数 } p_i \text{ の巡回群（} p_i \text{ は素数）}.$$

G_i に対応する体を K_i とすると, 次の図を得る：



K_i/K_{i-1} はガロア拡大でそのガロア群は G_i/G_{i-1} である. $p_1 \cdots p_{r-1} | n$ なので, K_{i-1} は 1 の原始 p_i 乗根を含み, 定理**??** により

$$K_i = K_{i-1}(\sqrt[p_i]{\alpha_i}), \quad \exists \alpha_i \in K_{i-1}, \quad K_1 = k(\zeta) = k(\sqrt[n]{1}).$$

更に, $K \subset K(\zeta) = K_r$ なので, $f(X) = 0$ は k 上代数的に解ける.

（必要性）$f(X)=0$ が k 上代数的に解けるとすると, 体の列

$$K_r \supset K_{r-1} \supset \cdots \supset K_0 = k$$

で

(1) $K_i = K_{i-1}(\alpha_i), \quad \alpha_i^{n_i} = a_i \in K_{i-1},$

(2) $K \subset K_r$

を満たすものが存在する.

K_r を含む k の最小のガロア拡大を L とする. すなわち, 補題 4.1.9 により, K_r から複素数体への k 上の埋め込み全体を

$$\mathrm{Emb}_k(K_r, \mathbb{C}) = \{\sigma_1, \cdots, \sigma_n\}$$

とするとき,

$$L = \sigma_1 K_r \cdot \cdots \cdot \sigma_n K_r$$

で与えられる. このとき, 各 l $(1 \leq l \leq n)$ に対し,

$$\sigma_l K_r \supset \sigma_l K_{r-1} \supset \cdots \supset K_0 = k, \quad \sigma_l K_i = (\sigma_l K_{i-1})(\sigma_l \alpha_i), \ (\sigma_l \alpha_i)^{n_i} = \sigma_l a_i \in \sigma_l K_{i-1} \tag{4.7}$$

を満たす. これらを順に積み上げることにより, L/k の中間体の列

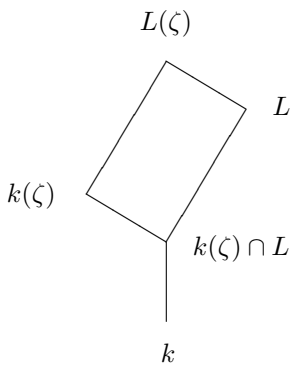
$$L = L_t \supset L_{t-1} \supset \cdots \supset L_0 = k$$

で

$$L_j = L_{j-1}(\gamma_j), \quad \gamma_j^{m_j} = c_j \in L_{j-1}$$

を満たすものを得る.

$m = m_1 \cdots m_t$ とし 1 の原始 m 乗根を ζ とする.



定理 4.1.11 により $L(\zeta)/k$ はガロア拡大である. また, 定理**??** により,

$$L_j(\zeta)/L_{j-1}(\zeta)$$

は巡回拡大で, その拡大次数は, m の約数である. $L_j(\zeta)$ に対応する $G := \mathrm{Gal}(L(\zeta)/k(\zeta))$ の部分群を G_j とすれば

$$G_0 = \{1\} \subset G_1 \subset \cdots \subset G_t = G$$

は

$$G_{j-1} \triangleleft G_j, \quad G_j/G_{j-1}\text{は巡回群}$$

を満たす. 従って G は可解群である. 更に 定理 4.1.3 により

$$\mathrm{Gal}(L(\zeta)/k) \triangleright \mathrm{Gal}(L(\zeta)/k(\zeta)) = G$$

であり

$$\mathrm{Gal}(L(\zeta)/k)/\mathrm{Gal}(L(\zeta)/k(\zeta)) \simeq \mathrm{Gal}(k(\zeta)/k).$$

$\mathrm{Gal}(k(\zeta)/k)$ は巡回群なので可解群である. 従って, 定理 1.7.15 により, $\mathrm{Gal}(L(\zeta)/k)$ も可解群であり, その剰余群 $\mathrm{Gal}(L/k)$ も可解群である. また $\mathrm{Gal}(K/k)$ は, $\mathrm{Gal}(L/k)$ の剰余群であるので, 可解群であり, K/k は可解拡大である. □

4.2.3　アーベルの定理

$K := k(X_1, \cdots, X_n)$ を体 k 上の n 変数有理関数体とする. 置換 $\sigma \in S_n$ と K の自己同型射

$$K \longrightarrow K; \quad f = f(X_1, \cdots, X_n) \longmapsto \sigma f = f(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$$

を同一視すると, S_n は, $\mathrm{Aut}(K)$ の部分群である. このとき, 不変体 K^{S_n} の元を **対称式** という. 多項式

$$S(T) = (T - X_1) \cdots (T - X_n) = T^n - s_1 T^{n-1} + \cdots + (-1)^n s_n \ \in K[T]$$

の係数 s_i を i 次 **基本対称式** という：

$$s_1 = X_1 + \cdots + X_n, \ s_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n, \ \cdots \ , \ s_n = X_1X_2 \cdots X_n.$$

体 K は分離多項式 $S(T)$ の $k(s_1, \cdots, s_n)$ 上の最小分解体なので, $K/k(s_1, \cdots, s_n)$ はガロア拡大で, そのガロア群は S_n の部分群である. 補題 4.1.6 より, K/K^{S_n} もガロア拡大で, そのガロア群は S_n である. 従って, $K^{S_n} = k(s_1, \cdots, s_n)$ でなければならない. よって, 次の定理を得る：

定理 4.2.2 任意の対称式は, 基本対称式の有理式として表される. 有理関数体 $K = k(X_1, \cdots, X_n)$ は $k(s_1, \cdots, s_n)$ のガロア拡大で, そのガロア群は S_n である.

体 F 上代数的に独立な n 個の元 $a_1, \cdots, a_n$ を係数とする n 次方程式

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n = 0$$

を **一般 n 次代数方程式** という.

$k = F(a_1, \cdots, a_n)$ とし, 多項式 $f(X)$ の k 上の最小分解体を K_f とする.

補題 4.2.3 ガロア拡大 K_f/k のガロア群 $\mathrm{Gal}(K_f/k)$ は n 次対称群 S_n に同形である.

証明 ガロア群 $\mathrm{Gal}(K_f/k)$ の元は, $f(X)$ の根の置換と見なせる. 即ち, $\sigma \in \mathrm{Gal}(K_f/k)$ に対し, $\sigma(\alpha_i) = \alpha_{\bar{\sigma}(i)}$ とする. このとき, $\bar{\sigma} \in S_n$ であり,

$$\phi : \mathrm{Gal}(K_f/k) \longrightarrow S_n; \quad \sigma \longmapsto \bar{\sigma}$$

は群単射である.

そこで, 任意の置換 $\tau \in S_n$ に対し, 環射

$$\xi : F[\alpha_1, \cdots, \alpha_n] \longrightarrow F[\alpha_1, \cdots, \alpha_n], \quad \xi(\alpha_i) = \alpha_{\tau(i)} \quad (1 \leq i \leq n)$$

が存在する. $f(X)$ の係数 a_i は, $f(X)$ の根の基本対称式なので, ξ は, $k = F(a_1, \cdots, a_n)$ 上の同型

$$k(\alpha_1, \cdots, \alpha_n) = K_f \longrightarrow K_f$$

を導く. 従って, $\xi \in \mathrm{Gal}(K_f/k)$ であり, $\phi(\xi) = \tau$. よって, ϕ は群同型射となり, $\mathrm{Gal}(K_f/k) \simeq S_n$ を得る. □

定理 4.2.4 （アーベルの定理）n 次一般代数方程式が代数的に解ける為の必要十分条件は $n \leq 4$ である.

証明 例 1.7.6 と 定理 1.7.18 により, S_n が可解群である為の必要十分条件は $n \leq 4$ である. 従って 定理 4.2.1 と 補題 4.2.3 とにより定理を得る. □

4.3 定規とコンパスによる作図

4.3.1 作図可能性と 2 冪拡大

(1) 定規による作図とは, 平面上に与えられた二点 P, Q $(P \neq Q)$ に対し, これら二点を通る直線を描くことである.

(2) コンパスによる作図とは, 平面上に与えられた二点 P, Q $(P \neq Q)$ に対し, P を中心とし Q を通る円を描くことである.

平面上に与えられた有限個の点 $P_1, \cdots, P_n$ から, 定規とコンパスによる作図で得られる点は次の何れかである.

二直線の交点, 直線と円との交点, 円と円との交点.

この操作を有限回繰返して得られる点を, $P_1, \cdots, P_n$ から **定規とコンパスにより作図可能な点** という.

以下平面 $\mathbb{R}^2$ 上の点 (x, y) に複素数 $x + yi$ を対応させて, $\mathbb{R}^2$ と $\mathbb{C}$ とを同一視する. 複素数 $\alpha = x + yi$ に対しその共役複素数 $x - yi$ を $\bar{\alpha}$ で表す.

次の補題の証明は, 演習問題とする.

補題 4.3.1 複素数 α, β が与えられたとき, 4 点 $0, 1, \alpha, \beta$ から, 複素数

$$\alpha + \beta, \quad -\alpha, \quad \alpha\beta, \quad \alpha^{-1}\ (\alpha \neq 0), \quad \bar{\alpha}$$

は作図可能である.

例 4.3.1 a を正の実数とする. 原点を中心とする半径 $a+1$ の円を C とする. 直線 $x = a - 1$ と円 C の交点の y 座標は $2\sqrt{a}$ である. 従って, $\sqrt{a}$ は作図可能である.

補題 4.3.2 $0, 1$ と複素数 α から, $\sqrt{\alpha}$ は作図可能である.

証明

$$|\alpha| = r, \quad \arg(\alpha) = \theta$$

とすれば

$$|\sqrt{\alpha}| = \sqrt{r}, \quad \arg(\sqrt{\alpha}) = \frac{\theta}{2}.$$

角の二等分と与えられた線分の平方根は作図可能であるから, $\sqrt{\alpha}$ は作図可能. □

次の補題の証明は演習問題とする.

補題 4.3.3 複素数 $\alpha, \beta\ (\alpha \neq \beta)$ に対し, これら二点を通る直線を $l(\alpha, \beta)$ で表す. また α を中心とし, β を通る円を $c(\alpha, \beta)$ で表す. このとき次が成り立つ.

(1) 複素数 $\alpha, \beta, \gamma, \delta\ (\alpha \neq \beta, \gamma \neq \delta)$ に対し, 二直線 $l(\alpha, \beta), l(\gamma, \delta)$ が平行でないならば, その交点は

$$\mathbb{Q}(\alpha, \beta, \gamma, \delta, \bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$$

に含まれる.

(2) 複素数 $\alpha, \beta, \gamma, \delta\ (\alpha \neq \beta, \gamma \neq \delta)$ に対し, 直線 $l(\alpha, \beta)$ と円 $c(\gamma, \delta)$ の交点は

$$\mathbb{Q}(\alpha, \beta, \gamma, \delta, \bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$$

の二次拡大体の元である.

(3) 複素数 $\alpha, \beta, \gamma, \delta\ (\alpha \neq \gamma, \alpha \neq \beta, \gamma \neq \delta)$ に対し, 二つの円 $c(\alpha, \beta), c(\gamma, \delta)$ の交点は

$$\mathbb{Q}(\alpha, \beta, \gamma, \delta, \bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$$

の二次拡大体の元である.

定理 4.3.4 $0, 1$ と n 個の複素数 $\alpha_1, \cdots, \alpha_n$ から, 複素数 α が定規とコンパスにより作図可能である為の必要十分条件は $\mathbb{C}$ の部分体の列

$$K = K_0 \subset K_1 \subset \cdots \subset K_N, \quad K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n, \bar{\alpha}_1, \cdots, \bar{\alpha}_n)$$

で, 次を満たすものが存在する事である：

(1) $\alpha \in K_N$.

(2) $[K_i : K_{i-1}] = 2 \quad (i = 1, \cdots, N)$.

証明 （十分性）補題 4.3.1 により, K のすべての元は, $0, 1, \alpha_1, \cdots, \alpha_n$ から作図可能である. K_{i-1} の元が全て作図可能とせよ. $[K_i : K_{i-1}] = 2$ なので $K_i = K_{i-1}(\sqrt{\beta_i})$ となる $\beta_i \in K_{i-1}$ が存在する. 補題 4.3.2 により, K_i のすべての元は作図可能である. よって帰納法により, K_N の全ての元は, $0, 1, \alpha_1, \cdots, \alpha_n$ から作図可能である.
（必要性） 補題 4.3.3 により, 作図可能な点は, 既知の体か, 或いはその二次拡大体に含まれる. □

4.3.2 正多角形の作図と角の三等分の作図不可能性

以下の議論では, 複素平面上に原点 O と点 1 は常に与えられているとする.

定理 4.3.5 正 n 角形が定規とコンパスによって作図可能である為には $\varphi(n) = 2^r$ となることが必要十分である. 但し, φ は Euler の関数である.

証明 正 n 角形を作図する事は, 1 の原始 n 乗根 $\zeta_n = e^{\frac{2\pi i}{2}}$ を作図する事に他ならない.
（必要性）定理 4.3.4 により, $\mathbb{C}$ の部分体の列

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_N$$

で

$$[K_i : K_{i-1}] = 2 \quad i = 1, \cdots, N, \quad \zeta_n \in K_N$$

なるものが存在する. このとき $[K_N : \mathbb{Q}]$ は 2 の巾である. 一方 ζ_n の最小多項式は n 次円分多項式 $\Phi_n(X)$ であり, その次数は $\varphi(n)$ である（定理 4.1.16）. 従って $\varphi(n) = 2^r$ でなければならない.
（十分性）$\varphi(n) = 2^r$ とすると, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ は次数 2^r のアーベル拡大である. 即ち $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = G$ は位数 2^r のアーベル群であるから, 部分群の列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

で

$$[G_i : G_{i+1}] = 2, \quad i = 0, 1, \cdots, r-1$$

となるものが存在する. G_i に対応する $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ の中間体を K_i とすれば

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r = \mathbb{Q}(\zeta_n)$$

で

$$[K_i : K_{i-1}] = 2, \quad \zeta_n \in K_r$$

を満たす. 従って 定理 4.3.4 により ζ_n は作図可能である. □

$m = 0, 1, 2, \cdots$ に対し,

$$F(m) = 2^{2^m} + 1$$

を m 次 **フェルマー数** といい, 素数であるフェルマー数を **フェルマー素数** という.

Fermat persisted in his conjecture‘‘ $F(m)$ は全て素数である ’’to the end of his days, usually adding that he had no proof for it.（A. Weil 著‘‘ Number Theory ’’p.58）

例 4.3.2

$$F(0)=3,\quad F(1)=5,\quad F(2)=17,\quad F(3)=257,\quad F(4)=65537$$

は素数であるが, ほぼ 100 年の後に Euler により $F(5)=4294967297=641\times 6700417$ と因数分解された. その後現在に至るまで, 5 次以上のフェルマー素数は見つかっていない.

系 4.3.6 $n=2^e p_1^{e_1}\cdots p_t^{e_t}$ を自然数 $n\,(\geq 2)$ の素因数分解とする. 正 n 角形が定規とコンパスによって作図可能である為には $e_1=\cdots=e_t=1$ で全ての p_i がフェルマー素数であることが, 必要十分である.

証明　例 2.3.8 により,

$$\varphi(n)=2^{e-1}p_1^{e_1-1}\cdots p_t^{e_t-1}(p_1-1)\cdots(p_t-1).$$

$\varphi(n)$ が 2 冪になる為には $e_1=\cdots=e_t=1$ で全ての p_i がフェルマー素数である事が, 必要十分である. □

特に

系 4.3.7 p を奇素数とするとき, 正 p 角形が定規とコンパスによって作図可能である為には p がフェルマー素数であることが, 必要十分である.

1796 年 3 月 30 日の朝, 18 才の Gauss により発見された正 17 角形の作図法と, それに纏わる物語については, 高木貞治著‘‘ 近世数学史談 ’’が白眉である.

例 4.3.3 正五角形は, 次のようにして作図される.

$$X=\zeta_5=\cos\phi+i\sin\phi,\quad \phi=\frac{2\pi}{5}$$

と表す. $\cos\phi$ が作図できれば, ζ_5 も作図できる. $X=\zeta_5$ は, $X^4+X^3+X^2+X+1=0$ を満たす. すなわち

$$X^2+X+1+\frac{1}{X}+\frac{1}{X^2}=0.$$

$Y=X+\frac{1}{X}=2\cos\phi$ とすれば, $Y^2+Y-1=0$. 従って $4\cos^2\phi+2\cos\phi-1=0$ となり

$$\cos\phi=\frac{\sqrt{5}}{4}-\frac{1}{4}.$$

$\sqrt{5}$ は作図可能であり, $\cos\phi$ は作図可能である.

定理 4.3.8（角の三等分）p を奇素数とするとき, 角の p 等分は一般には作図できない. 特に角の三等分は一般には作図できない.

証明　系 4.3.6 により, 正 p^2 角形は作図不可能である. 従って, 角 2π の p 等分と, 角 $\frac{2\pi}{p}$ の p 等分のどちらか一方は, 作図不可能である. □

第5章　環上の加群

環上の加群は, ベクトル空間, 加法群の一般化である. この章では, 環上の加群の基本的な概念を解説する.

5.1　加群と加群射

5.1.1　加群の定義と例

R を環とし, $(M;+)$ を 加法群とする. スカラー倍と呼ばれる写像

$$\cdot : R \times M \longrightarrow M, \quad (a, x) \longmapsto a \cdot x = ax$$

が定義され, 次を満たすとき, $(M;+,\cdot)$ を R **上の左加群**, または R**-左加群** という：

(M1) $1x = x \quad (\forall x \in M)$,

(M2) $(ab)x = a(bx) \quad (\forall a, b \in R, \forall x \in M)$,

(M3) $(a+b)x = ax + bx,\ a(x+y) = ax + ay \quad (\forall a, b \in R, \quad \forall x, y \in M)$.

同様にして, R**-右加群** が定義される. S も環とし, M が R-左加群であり同時に S-右加群とする.

$$(ax)b = a(xb) \quad (\forall a \in R,\ \forall x \in M,\ \forall b \in S)$$

が成り立つとき, M を (R, S)**-両側加群** という.

注意 5.1.1 R を可換環とし, M を R-左加群とする.

$$xa := ax \quad (a \in R,\ x \in M)$$

と定めることにより, M は, R-右加群となる.

左加群, 右加群の議論は平行に進められるので, 特に断らない限り, 専ら, R-左加群を取り扱い, 単に, R-加群という.

例 5.1.1 環 R 自身は, 乗法をスカラー倍とすることにより, (両側) R-加群である.

例 5.1.2 体 F 上の加群を F 上の **ベクトル空間**, または **線形空間** という.

例 5.1.3 M を加法群とする. $n \in \mathbb{Z}, x \in M$ に対し,

$$nx = |n|(\mathrm{sign}(n)x) \quad (\mathrm{sign}(0) = 1)$$

と定める. そこで,

$$\mathbb{Z} \times M \longrightarrow M; \quad (n, x) \longmapsto nx$$

をスカラー倍とすることにより, M は $\mathbb{Z}$-加群となる. すなわち, 加法群（アーベル群）と $\mathbb{Z}$-加群は同じものである.

例 5.1.4 $f : R \longrightarrow S$ を環射とし, M を S-加群とする.

$$R \times M \longrightarrow M, \quad (a, x) \longmapsto f(a)x$$

をスカラー倍とすることにより, M は R-加群となる.

5.1.2　部分加群, 剰余加群

M を R-加群とし, N を加法群 M の部分群とする.

$$a \in R,\ x \in N \quad \Longrightarrow \quad ax \in N$$

が満たされるとき, N を M の **部分** R-**加群** という. 即ち, R-加群 M の部分集合 N が部分加群である為の必要十分条件は, M に於ける和とスカラー倍から導かれる和とスカラー倍により, N が R-加群となることである.

例 5.1.5 N を加法群 M の部分群とする. このとき, N は $\mathbb{Z}$-加群 M の 部分 $\mathbb{Z}$-加群である.

例 5.1.6 環 R の部分 R-左加群は R の左イデアルに他ならない.

R-加群 M の元 $x_1, \cdots, x_n$ に対し, M の元

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \quad (a_i \in R\ (1 \leq i \leq n))$$

を, $x_1, x_2, \cdots, x_n$ の R 係数 **一次結合** という.

M を R-加群とし, $S = \{x_i\}_{i \in I}$ を M の部分集合とする. S に含まれる元の R 係数一次結合全体は, S を含む, M の最小の部分加群であり, これを $\langle S \rangle$ または

$$\sum_{i \in I} Rx_i$$

と表す. $M = \langle S \rangle$ となるとき, S は M を **生成する** という. $S = \{x_1, \cdots, x_n\}$ のとき, M は **有限生成である** といい, $M = Rx_1 + \cdots + Rx_n$ と表す.

例 5.1.7 M が有限生成 R-加群とする. このとき, M の部分加群 M' が有限生成とは限らない. 例えば, 体 k 上の無限変数多項式環 $R = k[X_1, X_2, \cdots]$ において, R 自身は, R-加群として有限生成であるが, その部分加群 $\langle \{X_1, X_2, \cdots\} \rangle$ は, 有限生成ではない.

例 5.1.8 M を環 R 上の加群とし, $\{N_\lambda\}_{\lambda\in\Lambda}$ を, M の部分加群の集まりとする.

$$\sum_{\lambda\in\Lambda} N_\lambda := \langle \cup_\lambda N_\lambda \rangle$$

を, 部分加群 $\{N_\lambda\}$ の**和** という.

例 5.1.9 R を環とし, $\mathfrak{a}$ を左イデアルとする. M を R-加群とするとき,

$$\mathfrak{a}M := \{a_1x_1 + \cdots + a_nx_n \mid a_i \in \mathfrak{a},\ x_i \in M\}$$

は, M の部分加群である. $\mathfrak{b}$ も左イデアルとすると,

$$(\mathfrak{a}\mathfrak{b})M = \mathfrak{a}(\mathfrak{b}M), \quad (\mathfrak{a}+\mathfrak{b})M = \mathfrak{a}M + \mathfrak{b}M$$

が成り立つ.

N を R-加群 M の部分加群とする. 加法群としての剰余群 M/N に対し,

$$[x] = [y] \quad \Longrightarrow \quad [ax] = [ay]\ (\forall a \in R)$$

が成り立ち, 写像

$$\cdot : R \times (M/N) \longrightarrow M/N; \quad (a, [x]) \longmapsto a \cdot [x] = a[x] := [ax]$$

が定義される. すると, $(M/N; +, \cdot)$ は R-加群をなし, M を N で割った **剰余加群** と呼ばれる.

問 5.1.1 $(M/N; +, \cdot)$ が R-加群をなすことを確かめよ.

例 5.1.10 R を可換環, $\mathfrak{m}$ をその極大イデアルとし, M を R-加群とする. $\mathfrak{m}M$ は M の部分加群であり,

$$R/\mathfrak{m} \times M/\mathfrak{m}M \longrightarrow M/\mathfrak{m}M, \quad ([a], [x]) \mapsto [ax]$$

は Well-defined である, 即ち, 剰余類 $[ax]$ は剰余類 $[a]$, $[x]$ の代表元 a, x の取り方によらず定まる. この写像をスカラー倍として, $M/\mathfrak{m}M$ は, 体 $R/\mathfrak{m}$ 上のベクトル空間となる.

5.1.3 加群射

R を環とし, M, N を R-加群とする. 加法群としての群射 $f : M \longrightarrow N$ が

$$f(ax) = af(x) \quad (\forall a \in R,\ \forall x \in M)$$

を満たすとき, f を R-**加群射**[1] という. R-同型射, R-同型, 核などの定義も, 加法群の場合に準ずる.

例 5.1.11 加法群としての群射 $f : G \longrightarrow H$ は $\mathbb{Z}$-加群射である.

[1] R-**準同型写像** または R-**線形写像** ともいう.

例 5.1.12 N を R-加群 M の部分加群とする.

$$\iota : N \longrightarrow M; \quad x \longmapsto x, \quad \pi : M \longrightarrow M/N; \quad x \longmapsto [x]$$

を, それぞれ, **自然な加群単射, 自然な加群全射** という.

問 5.1.2 $f : M \longrightarrow N$, $g : N \longrightarrow L$ が R-加群射ならば, $g \circ f$ も R-加群射であることを示せ.

問 5.1.3 $f : M \longrightarrow N$ を R-加群射とする. $\mathrm{Ker}(f) = \{0\}$ は, f が加群単射であるための必要十分条件であることを示せ.

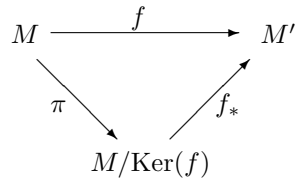
次の定理は, 群または環の場合と同様にして, 証明されるので, その証明を略す：

定理 5.1.4 $f : M \longrightarrow M'$ を R-加群射とするとき, 次が成り立つ：

(1) N が M の部分加群ならば, $f(N)$ は M' の部分加群である.

(2) N' が M' の部分加群ならば, $f^{-1}(N')$ は M の部分加群である.

(3) （加群射の分解定理）次の図を可換にする R-加群単射 $f_* : M/\mathrm{Ker}(f) \longrightarrow M'$ が一意的に存在する：



ただし $\pi : M \longrightarrow M/\mathrm{Ker}(f)$ は自然な加群全射である.

(4) （同型定理）特に, $f : M \longrightarrow M'$ が R-加群全射ならば, $M/\mathrm{Ker}(f) \simeq M'$.

(5) （対応定理）M の $\mathrm{Ker}(f)$ を含む部分加群 N と $\mathrm{Im}(f)$ の部分加群 N' は,

$$N' = f(N), \quad N = f^{-1}(N')$$

により, 1 対 1 に対応し,

$$M/N \simeq (M/\mathrm{Ker}(f))/(N/\mathrm{Ker}(f)) \simeq \mathrm{Im}(f)/N'.$$

R-加群射の（有限または無限の）列

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

は

$$\mathrm{Ker}(f_i) = \mathrm{Im}(f_{i-1}) \quad (\forall i)$$

を満たすとき, **完全系列**, または **完全列** と呼ばれる.

例 5.1.13 $O=\{0\}$ とする. このとき, 次が成り立つ：

$$\begin{array}{lll} O\longrightarrow M\longrightarrow O & (\text{完全}) & \Longleftrightarrow \quad M=O \\ O\longrightarrow M\xrightarrow{f} M' & (\text{完全}) & \Longleftrightarrow \quad f:\ \text{単射} \\ M\longrightarrow M'\xrightarrow{f} O & (\text{完全}) & \Longleftrightarrow \quad f:\ \text{全射} \\ O\longrightarrow M\xrightarrow{f} M'\longrightarrow O & (\text{完全}) & \Longleftrightarrow \quad f:\ \text{同型射} \end{array}$$

問 5.1.5 上の例を確かめよ.

R-加群射の完全列

$$O\longrightarrow M'\xrightarrow{f} M\xrightarrow{g} M''\longrightarrow O \tag{5.1}$$

を, 特に, **短完全列** という.

命題 5.1.6 (5.1) に於いて, 次は同値である：

(1) $g\circ h=I_{M''}$ を満たす R-加群射 $h: M''\longrightarrow M$ が存在する.

(2) M の部分加群 N で

$$M=f(M')+N,\quad f(M')\cap N=O$$

を満たすものが存在する.

(3) $k\circ f=I_{M'}$ を満たす R-加群射 $k: M\longrightarrow M'$ が存在する.

証明 (1) $\Longrightarrow$ (2) $N=h(M'')$ とおくと, $M=f(M')+N, f(M')\cap N=O$ を満たす. (2) $\Longrightarrow$ (1) $g|_N: N\longrightarrow M'$ は同型射なので, $h=(g|_N)^{-1}$ とすれば, $g\circ h=I_{M''}$. (2) $\Longleftrightarrow$ (3) は演習問題とする. □

命題の条件が成り立つとき, (5.1) は **分裂する** という.

問 5.1.7 命題 5.1.6 に於ける (2) $\Longleftrightarrow$ (3) の証明をせよ.

5.2 直積, 直和, 自由加群

5.2.1 直積と直和

R を環とし, $\{M_i|i\in I\}$ を R-加群の集合とする. 加法群としての直積 $\prod_{i\in I}M_i$ に対し,

$$\cdot: R\times\prod_{i\in I}M_i\longrightarrow\prod_{i\in I}M_i;\quad (a,(x_i)_{i\in I})\longmapsto(ax_i)_{i\in I}$$

とするとき, $(\prod_{i\in I}M_i;+,\cdot)$ は R-加群をなす. これを $\{M_i\}$ の **直積（加群）** という. 各 $j\in I$ に対し, 写像

$$\pi_j:\prod_{i\in I}M_i\longrightarrow M_j;\quad (\cdots,x_j,\cdots)\longmapsto x_j$$

は, R-加群全射であり, j 番目の **射影** と呼ばれる.

直積の元で有限個の成分のみが 0 と異なるもの全体のなす部分加群

$$\bigoplus_{i\in I} M_i$$

を $\{M_i\}$ の **直和（加群）** といい, R-加群単射

$$\iota_j : M_j \longrightarrow \bigoplus M_i; \quad x_j \longmapsto (\cdots, 0, x_j, 0, \cdots)$$

を j 番目の **入射** という.

有限個の R-加群の直積と直和は同じものである. M を R-加群とし, $\{N_i \mid i \in I\}$ を M の部分加群の集合とする. R-加群射

$$f : \bigoplus_{i\in I} N_i \longrightarrow M; \quad (x_i) \longmapsto \sum x_i$$

の像は部分加群の和 $\sum_{i\in I} N_i$ に一致する. f が同型射のとき, M は **部分加群** $\{N_i\}$ **の直和**であるといい,

$$M = \bigoplus_{i\in I} N_i$$

と表す.

5.2.2　自由加群

M を R-加群とし, $\{x_1, \cdots, x_n\} \subset M$ とする.

$$a_1x_1 + \cdots + a_nx_n = 0 \ (a_i \in R) \quad \Longrightarrow \quad a_1 = \cdots = a_n = 0$$

が成り立つとき, $\{x_1, \cdots, x_n\}$ は, R 上, **一次独立である** という.

S を M の部分集合とする. S の空でない任意の有限部分集合が一次独立であるとき, S は **一次独立である** という.

$M = \langle S \rangle$ を満たす一次独立である部分集合 S を M の **基底** という. 基底 S を持つ R-加群を **自由加群** といい, $\mathrm{card}(S)$ をその **階数** という. 零加群 $O = \{0\}$ も便宜上, 階数 0 の自由加群という. 自由 $\mathbb{Z}$-加群を **自由アーベル群** という.

例 5.2.1 一般の加群には, 基底が存在するとは限らない. 例えば, $\mathbb{Z}$-加群 $\mathbb{Z}/(n)$ $(n > 0)$ には, $\mathbb{Z}$ 上一次独立な元は存在しない. 従って基底も存在しない.

定理 5.2.1 R-加群 F に対し次は同値である：

(1) F は自由加群である.

(2) $F \simeq \oplus_{i\in I} R_i, \quad \exists I \ (R_i = R \ , \ \forall i)$.

証明 (1) $\Longrightarrow$ (2) $S = \{x_i\}_{i\in I}$ を F の基底とする.

$$\phi : \bigoplus_{i\in I} R \longrightarrow F; \quad (a_i)_i \longmapsto \sum_i a_i x_i$$

は R-加群同型射である. (2) $\Longrightarrow$ (1) i 番目の入射 $\iota_i : R \longrightarrow \oplus_i R$ に対し,

$$e_i := \iota_i(1) = (\cdots, 0, 1, 0 \cdots)$$

とおく. このとき, $\{e_i\}_{i\in I}$ は $\oplus_i R$ の基底であり, $\oplus_i R$ は自由加群である. □

注意 5.2.1 $\{e_i\}_{i\in I}$ を $\oplus_i R$ の **標準基底** という.

次の定理は, 自由加群を特徴付けるものである：

定理 5.2.2 F は $\{e_i\}_{i\in I}$ を基底とする自由 R 加群とする. 任意の R-加群 M と任意の部分集合 $S = \{x_i\}_{i\in I}$ に対し, $f(e_i) = x_i$ $(\forall i)$ を満たす加群射 $f : F \longrightarrow M$ が唯一つ存在する. 特に, 任意の R 加群 M に対し, 自由加群 F と加群全射 $f : F \longrightarrow M$ が存在する.

証明 F の任意の元は $a_{i_1}e_{i_1} + \cdots + a_{i_n}e_{i_n}$ と表される. そこで, $f(\sum\ a_{i_\alpha}e_{i_\alpha}) = \sum a_{i_\alpha}x_{i_\alpha}$ とする. このとき, f が求める加群射であり, その一意性は明らかである. □

問 5.2.3 階数が等しい二つの自由加群は同型であることを示せ.

定理 5.2.4 体 K 上のベクトル空間 V は自由加群である. 即ち, V は基底を持つ. さらに, 基底の濃度は, 基底の取り方に依らず一定である.

証明 $V = O = \{0\}$ のときは良い. $V \neq O$ のとき, Zorn の補題を用いて, 基底の存在を示す. V の一次独立な部分集合全体のなす集合を $\mathcal{S}$ と表すと, 包含関係に関し, $\mathcal{S}$ は順序集合である. $0 \neq x \in V$ に対し, $\{x\}$ は一次独立である. 特に, $\mathcal{S} \neq \emptyset$. $\{S_i\}_{i\in I}$ を $\mathcal{S}$ の全順序部分集合とするとき, $\cup_{i\in I} S_i$ は, その上限である. よって, $\mathcal{S}$ は空でない帰納的順序集合であり, Zorn の補題により, $\mathcal{S}$ は極大元 S_0 を持つ. このとき, S_0 は, その極大性により, $V = \langle S_0\rangle$ が成り立ち, V の基底である.

次に基底の濃度が一定であることを示す. S, T を共に V の基底であるとする. 次の補題により, S が無限集合ならば, T も無限集合であり, $\mathrm{card}(S) = \mathrm{card}(T)$ を得る. そこで, S, T が共に有限集合の場合を示せば良い.

$$S = \{u_1, \cdots, u_m\}, \quad T = \{v_1, \cdots, v_n\}$$

を基底とし, $m < n$ と仮定しよう. このとき, $0 \leq k \leq m$ に対し, T の基底の番号を適当に付け替えると,

$$\{u_1, \cdots, u_k, v_{k+1}, \cdots, v_n\}$$

が, V の基底となることを, k に関する帰納法で示す. $k = 0$ のときは明らかで, k のときを仮定する. すると,

$$u_{k+1} = a_1u_1 + \cdots + a_ku_k + a_{k+1}v_{k+1} + \cdots + a_nv_n \quad (a_i \in K)$$

と表される.

$$a_{k+1} = \cdots = a_l = 0,\ a_l \neq 0$$

と仮定する. このとき,

$$\{u_1, \cdots, u_{k+1}, v_{k+1}, \cdots, v_{l-1}, v_{l+1}, \cdots, v_n\}$$

は V の基底である. よって, 上の主張は示された.

主張に於いて, $k = m$ とすれば明らかに不合理である. よって, $m \geq n$ を得る. 同様にして, $n \geq m$ を得て, $m = n$ を得る. □

補題 5.2.5 M を環 R 上の自由加群とする. $\{x_i\}_{i\in I}$, $\{y_j\}_{j\in J}$ を二組の基底とする. I が無限集合ならば, $\mathrm{card}(I) = \mathrm{card}(J)$, 即ち, I から J への全単射が存在する

証明 $S = \{x_i\}_{i\in I}$, $T = \{y_j\}_{j\in J}$ とする. 任意の x_i は T の元の一次結合として表されるので, 空でない有限部分集合 $J(i) \subset J$ が存在し

$$x_i = \sum_{j\in J(i)} a_j y_j \quad (a_j \in R)$$

と表される. このとき, $\cup_{i\in I}\{y_j \mid j \in J(i)\}$ は基底である. よって $J = \cup_{i\in I} J(i)$ が成り立つ. 同様にして, $I = \cup_{j\in J} I(j)$ と表される. 特に, I が無限集合なので, J も無限集合である.

I は無限集合なので, $\aleph_0 \leq \mathrm{card}(I)$, $\mathrm{card}(I)^2 = \mathrm{card}(I)$ が成り立つことに注意する. 従って,

$$\mathrm{card}(J) = \mathrm{card}(\cup_{i\in I} J(i)) \leq \mathrm{card}(I)\aleph_0 \leq \mathrm{card}(I)^2 = \mathrm{card}(I)$$

を得る. J も無限集合なので, 同様にして, $\mathrm{card}(I) \leq \mathrm{card}(J)$ を得る. よって, $\mathrm{card}(I) = \mathrm{card}(J)$ が成り立つ. □

定理 5.2.6 R を可換環とし, M を R-加群とする. $\{x_1, \cdots, x_n\}, \{y_1, \cdots, y_m\}$ が, 共に, 基底ならば, $n = m$ が成り立つ.

証明 $\mathfrak{m}$ を R の極大イデアルとすると, 補題 2.5.5 により, 剰余環 $K := R/\mathfrak{m}$ は体である. $\mathfrak{m}M$ は M の部分加群であり, 自然な加群全射 $\pi : M \longrightarrow M/\mathfrak{m}M$ を考える. 例 5.1.10 で見たように, $M/\mathfrak{m}M$ は体 K 上のベクトル空間となる. このとき,

$$\{\pi(x_1), \cdots, \pi(x_n)\}, \quad \{\pi(y_1), \cdots, \pi(y_n)\}$$

は K 上のベクトル空間 $M/\mathfrak{m}M$ の二組の基底となる. これを示そう.

$a \in R$ の定める $K = R/\mathfrak{m}$ の元を $\bar{a}$ と表す.

$$\overline{r_1}\pi(x_1) + \cdots + \overline{r_n}\pi(x_n) = 0, \quad r_i \in R$$

とすると

$$r_1x_1 + \cdots + r_nx_n \in \mathfrak{m}M.$$

従って

$$r_1x_1 + \cdots + r_nx_n = b_1x_1 + \cdots + b_nx_n, \quad b_i \in \mathfrak{m}$$

と表される. $\{x_i\}$ は基底なので

$$r_1 = b_1, \cdots, r_n = b_n$$

である. 従って $\overline{r_1} = \cdots = \overline{r_n} = 0$ となり $\{\pi(x_1), \cdots, \pi(x_n\}$ は K 上一次独立である. また $\{\pi(x_i)\}$ が $M/\mathfrak{m}M$ を生成するのは明らかなので, これは基底である. 同様に $\{\pi(y_j)\}$ も $M/\mathfrak{m}M$ の基底である. ベクトル空間の場合の結果を用いて $n = m$ を得る. □

補題 5.2.7 $f : M \longrightarrow N$ を R-加群全射とする. F を自由加群とし, $\phi : F \longrightarrow N$ を R-加群射とする. このとき, R-加群射 $\psi : F \longrightarrow M$ で, $f \circ \psi = \phi$ を満たすものが存在する.

証明 $F = \oplus_{i \in I} R$ としてよい. $\{e_i\}$ を標準基底とし, $\phi(e_i) = y_i \in N$ とする. f は全射なので, $f(x_i) = y_i$ となる $x_i \in M$ が存在する. そこで, $\psi(e_i) = x_i$ とすれば, $\psi : F \longrightarrow M$ が求めるものである. □

5.2.3 自由加群の加群射と行列

この小節では, 可換環 R 上の階数有限な自由加群を取り扱う. R-加群射の行列表示を考える際には, **基底は順序のついた列** とする.

M, N を階数 m, n の自由 R-加群とし, $\mathcal{B} = (x_1, \cdots, x_m), \mathcal{C} = (y_1, \cdots, y_n)$ をそれらの基底とする. R-加群射 $f : M \longrightarrow N$ に対し,

$$f(x_j) = \sum_{i=1}^{n} a_{ij} y_i \quad A := (a_{ij}) \in R^{n \times m}$$

とする:

$$f\mathcal{B} := (f(x_1), \cdots, f(x_m)) = (y_1, \cdots, y_n)A = \mathcal{C}A.$$

同型写像

$$\phi : R^m = R^{m \times 1} \longrightarrow M, \quad \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \longmapsto \sum_{i=1}^{m} r_i x_i = (x_1, \cdots, x_m) \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix},$$

$$\psi : R^n \longrightarrow N, \quad \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \longmapsto \sum_{j=1}^{n} s_j y_j = (y_1, \cdots, y_n) \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$$

に対し,

$$f(\phi({}^t(r_1, \cdots, r_m))) = \psi(A\,{}^t(r_1, \cdots, r_n)).$$

即ち, 次の図は可換である:

$$\begin{array}{ccc} & A & \\ R^m & \longrightarrow & R^n \\ \phi \downarrow & & \downarrow \psi \\ M & \longrightarrow & N \\ & f & \end{array}.$$

但し, 行列 A は, 写像

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \longmapsto A \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix}$$

を表す. 行列 $A = A(f)$ を基底 $\mathcal{B}$,$\mathcal{C}$ に関する f の **表現行列** という：

$$f\mathcal{B} = \mathcal{C}A. \tag{5.2}$$

定理 5.2.8 M, N を階数 m, n の自由加群とし, $\mathcal{B} = (x_1, \cdots, x_m)$, $\mathcal{C} = (y_1, \cdots, y_n)$ をそれぞれの基底とする. 加群射 $f : M \longrightarrow N$ に対し, $\mathcal{B}$,$\mathcal{C}$ に関する f の表現行列を $A(f)$ と表すことにすると,

$$\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{M}_{n\times m}(R); \quad f \longmapsto A(f)$$

は, R-加群同型射である. 更に次が成り立つ：

(1) f は加群単射 $\Longleftrightarrow$ $\{f(x_i)\}$ は一次独立 $\Longleftrightarrow$ $A(f)$ の列ベクトルは一次独立.

(2) f は加群全射 $\Longleftrightarrow$ $\{f(x_i)\}$ は N を生成する $\Longleftrightarrow$ $A(f)$ の列ベクトルは R^n を生成する.

(3) f は加群同型射 $\Longleftrightarrow$ $\{f(x_i)\}$ は基底をなす $\Longleftrightarrow$ $A(f)$ の列ベクトルは R^n の基底をなす.

系 5.2.9 M を階数 n の自由加群とし, $\mathcal{B}$ をその基底とする. M から M への線形写像 f に対し, $\mathcal{B}$ に関する f の表現行列を $A(f)$ と表すことにすると,

$$\mathrm{End}_R(M) \longrightarrow \mathrm{M}_n(R); \quad f \longmapsto A(f)$$

は, R-代数の同型射である.

問 5.2.10 定理 5.2.8 を確かめよ.

次に, 自由加群の基底を取り替えたとき, 表現行列がどう変わるかを調べる. M, N を階数 n, m の自由加群とし, $\mathcal{B}$,$\mathcal{B}'$ を M の基底, $\mathcal{C}$,$\mathcal{C}$ を N の基底とする. このとき,

$$\mathcal{B}' = \mathcal{B}P, \quad \mathcal{C}' = \mathcal{C}Q$$

を満たす, $P \in \mathrm{GL}_n(R), Q \in \mathrm{GL}_m(R)$ が存在する. 線形写像 f に対し, $\mathcal{B}$,$\mathcal{C}$ に関する f の表現行列を $A(f)$ と表すと,

$$f\mathcal{B}' = f\mathcal{B}P = \mathcal{C}A(f)P, \quad \mathcal{C}'Q^{-1} = \mathcal{C}$$

であり,

$$f\mathcal{B}' = \mathcal{C}'Q^{-1}A(f)P.$$

従って, f の基底 $\mathcal{B}'$,$\mathcal{C}'$ に関する表現行列は $Q^{-1}A(f)P$ となる.

命題 5.2.11 V,W を体 k 上, 次元 m,n の線形空間とし, $\mathcal{B}=(u_1,\cdots,u_m)$, $\mathcal{C}=(v_1,\cdots,v_n)$ をそれぞれの基底とする. 線形射 $f:V\longrightarrow W$ に対し, $\mathcal{B},\mathcal{C}$ に関する f の表現行列を $A(f)$ と表す. このとき, 次が成り立つ：

(1) $\mathrm{Ker}(f)\simeq\{x\in k^n\mid A(f)x=0\}$.

(2) $\dim_k\mathrm{Im}(f)=\mathrm{rank}\ A(f)$.

(3) $m=\dim V=\dim_k(\mathrm{Ker}\ f)+\dim_k(\dim\ f)$.

問 5.2.12 上の命題を証明せよ.

5.3 有限性と半単純性

5.3.1 有限条件

R を環とし, M を有限生成 R-加群とする. すると, 非負整数 m と加群全射 $g:R^m\longrightarrow M$ が存在する. 従って, 同型定理により, $R^m/\mathrm{Ker}(g)\simeq M$. $\mathrm{Ker}(g)$ が有限生成ならば, 再び, 非負整数 n と加群全射 $f:R^n\longrightarrow\mathrm{Ker}(g)$ が存在する. f と自然な加群単射 $\mathrm{Ker}(g)\longrightarrow R^m$ の合成写像を, 改めて, f と表すと完全系列

$$R^n\xrightarrow{f}R^m\xrightarrow{g}M\longrightarrow O$$

を得る. R-加群射 f は, ある行列 $A\in\mathrm{M}_{m\times n}(R)$ が存在し, $f(X)=AX$ $(\forall X\in R^n)$ と表され, $M\simeq\mathrm{Coker}(f)$. 言い換えると, 行列 A の各列ベクトル $A_1,\cdots,A_n$ の生成する R^m の部分加群が, $\mathrm{Im}(f)$ であり, $M\simeq R^m/\mathrm{Im}(f)=\mathrm{Coker}(f)$ となる. 従って, 有限生成 R-加群の構造が, 行列 A により記述される.

上の議論で肝腎なことは, R^m の部分加群 $\mathrm{Ker}(g)$ が有限生成となることである. R^m は有限生成 R-加群であるが, その部分加群が有限生成となる保証はない. そこで, Noether 加群の概念に至る.

命題 5.3.1 M を R-加群とするとき, 次は同値である.

(1) M の任意の部分加群は有限生成である.

(2) $M_1\subset M_2\subset\cdots$ を部分加群の増大列とする. このとき, ある n が存在して, $M_n=M_{n+1}=\cdots$.

(3) $\mathcal{S}$ を M の部分加群の空でない集合とする. このとき, $\mathcal{S}$ には, 包含関係を順序として, 極大元が存在する.

証明 M の部分加群全体の集合は, 包含関係により, 順序集合 $\mathcal{M}$ をなす. (2), (3) を, それぞれ, 順序集合 $\mathcal{M}$ の　鎖律, 極大条件という. まず, (2) と (3) が同値であることを示そう.

極大元を持たない M の部分加群の空でない集合 $\mathcal{S}$ が存在したと仮定する. このとき, 各 $N\in\mathcal{S}$ に対し, $\mathcal{S}_N:=\{N'\in\mathcal{S}\mid N\subset N'\}\neq\emptyset$ である. すると, 選出公理により, $f(N)\in\mathcal{S}_N$ $(\forall N)$ を満たす写像 $f:\mathcal{S}\longrightarrow\mathcal{M}$ が存在する. $M_1\in\mathcal{S}$ を任意にとり,

$$f(M_1)=M_2,\cdots,f(M_n)=M_{n+1},\cdots$$

とすると, $\{M_n\}$ は部分加群の真の増大列となる. よって, (2) $\Longrightarrow$ (3) が示された. 逆に, M の部分加群の真の増大列 $\mathcal{S} = \{M_n \mid n \in \mathbb{N}\}$ が存在したとすると, $\mathcal{S}$ は極大元を持たない. よって, (3) $\Longrightarrow$ (2) が示された.

次に, (1) と (2) が同値であることを示そう. $\{M_n \mid n \in \mathbb{N}\}$ を M の部分加群の真の増大列とする. このとき,

$$N := \cup_{i=1}^{\infty} M_i$$

は, M の部分加群である. (1) を仮定すると, $N = Rx_1 + \cdots + Rx_k$ $(x_i \in N)$ と表される. $x_1, \cdots, x_k \in M_n$ とすれば, $N = M_n = M_{n+1} = \cdots$ となり, (2) を得る.

今度は, (2) を仮定し, N を M の部分加群とする. $N = O$ ならば明白. $N \neq O$ ならば $\exists x_1 \ (\neq 0) \in N$. $N = Rx_1$ ならば証明終. $Rx_1 \subsetneq N$ ならば $\exists x_2 \in N \backslash Rx_1$. $N = Rx_1 + Rx_2$ ならば証明終. これを何度か繰り返せば, $N = Rx_1 + \cdots + Rx_n$ となり, N は有限生成である. さもなければ, 部分加群の真の増大列

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq \cdots$$

が得られ, (2) に反する. □

命題の条件を満たす加群を極大条件を満たす加群, または **Noether 加群** という.

命題 5.3.2　(1) R-加群の短完全列

$$O \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow O$$

に対し,

$$M \text{ ：Noether 加群} \quad \Longleftrightarrow \quad M',\ M'' \text{ ：Noether 加群.}$$

(2) Noether 加群の有限個の直和は Noether 加群である.

証明　(1) ($\Longrightarrow$) 明白. ($\Longleftarrow$) $M_1 \subset M_2 \subset \cdots$ を M の部分加群の増大列とする. $\pi : M \longrightarrow M/M'$ を自然な加群全射とするとき, 仮定により, 適当な n が存在し

$$M_n \cap M' = M_{n+1} \cap M' + \cdots, \quad \pi(M_n) = \pi(M_{n+1}) = \cdots$$

を満たす. $l \geq n$ に対し,

$$O \longrightarrow M_l \cap M' \longrightarrow M_l \longrightarrow \pi(M_l) \longrightarrow O$$

は短完全列なので, $M_n = M_{n+1} = \cdots$ を得る.
(2) は (1) から, 帰納法を用いて, 容易に得られる. □

定理 5.3.3　M を Noether 環 R 上の有限生成加群とする. このとき M は Noether 加群である.

証明　M は有限生成 R-加群なので, 加群全射 $R^n \longrightarrow M$ が存在する. R は R-加群として, Noether 加群である. 従って, 命題 5.3.2 から, R^n も Noether 加群であり, その剰余加群も Noether 加群である. □

包含関係を逆にして, 次の命題を得る：

命題 5.3.4 M を R-加群とするとき, 次は同値である.

(1) $M_1 \supset M_2 \supset \cdots$ を部分加群の減少列とする. このとき, ある n が存在して, $M_n = M_{n+1} = \cdots$.

(2) $\mathcal{S}$ を M の部分加群の空でない集合とする. このとき, $\mathcal{S}$ には, 包含関係を順序として, 極小元が存在する.

命題の条件を満たす加群を極小条件を満たす加群, または **Artin 加群** という.

命題 5.3.5 (1) R-加群の短完全列

$$O \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow O$$

に対し,

$$M \text{ ：Artin 加群} \iff M',\ M'' \text{ ：Artin 加群.}$$

(2) Artin 加群の有限個の直和は Artin 加群である.

5.3.2 完全可約加群

M を O と異なる R-加群とする. M の部分加群が自明な O と M に限るとき, M を **単純加群**, または **既約加群** という.

定理 5.3.6 (Schur の補題) M, N を既約加群とするとき, 0 と異なる加群射 $f : M \longrightarrow N$ は同型射である. 特に, M の自己準同型環 $E_R(M)$ は斜体をなす.

証明 $\mathrm{Ker}(f)$, $\mathrm{Im}(f)$ は, それぞれ, M N の部分加群である. $f \neq 0$ より, $\mathrm{Ker}(f) = O$, $\mathrm{Im}(f) = N$ を得る. よって, f は全単射であり, 同型射である. □

既約な加群の直和として表される加群を **半単純加群**, または **完全可約加群** という. また, 直和因子を持たない加群を **直既約加群** という.

補題 5.3.7 R-加群 $M \neq O$ は既約な部分加群を持つ.

証明 $0 \neq x \in M$ をとる. このとき, 加群射

$$f : R \longrightarrow Rx; \quad r \longmapsto rx$$

の核 $\mathrm{Ker}(f)$ は R の真の左イデアルである. すると, Zorn の補題により, $\mathrm{Ker}(f)$ を含む極大な左イデアル $\mathfrak{m}$ が存在する. このとき, $\mathfrak{m}x$ は Rx の極大部分加群である. $M = \mathfrak{m}x \oplus M'$ とおくと, $Rx = \mathfrak{m}x \oplus (N' \cap Rx)$ が成り立つ. 実際, $y \in Rx$ を, $y = mx + y'$ $(m \in \mathfrak{m}, y' \in M'$ と表すとき, $y' = y - mx \in Rx \cap M'$ となる. $\mathfrak{m}x$ は Rx の極大部分群なので, $M' \cap Rx$ は既約加群である. □

定理 5.3.8 R-加群 M に対し, 次は同値である：

(1) M は既約加群の和である.

(2) M は完全可約加群.

(3) M の任意の部分加群は直和因子.

補題 5.3.9 $\{M_i\}_{i\in I}$ を M の既約部分加群の集合とする. $M=\sum_{i\in I}M_i$ ならば, 部分集合 $J\subset I$ が存在して, $M=\oplus_{j\in J}M_j$ が成り立つ.

証明　Zorn の補題により,

$$\sum_{j\in J}M_j=\oplus_{j\in J}M_j$$

を満たす極大な $J\subset I$ が存在する. このとき, $M=\sum_{j\in J}M_j$ が成り立つことを示す. 任意の M_i をとる. $i\in J$ ならば, $M_i\subset\sum_{j\in J}M_j$. $i\notin J$ とすると, J の極大性より, $M_i\cap\sum_{j\in J}M_j\neq O$ であり, M_i の部分加群である. M_i は既約なので, $M_i\subset\sum_{j\in J}M_jM_J$. 従って, $M=\sum_{j\in J}M_j=\oplus_{j\in J}M_j$ となる. □

定理の証明 (1) $\Longrightarrow$ (2) これは補題に他ならない. (2) $\Longrightarrow$ (3) N を M の部分加群とし, $N+(\oplus_{j\in J}M_j)$ が直和になる, 即ち, $N\cap(\oplus_{j\in J}M_j)=O$ となる極大な部分集合 $J(\subset I)$ をとる. このとき, 補題の証明と同様にして, $M=N\oplus(\oplus_{j\in J}M_j)$ を得る.

(3) $\Longrightarrow$ (1) $M\neq O$ として良い. M の全ての既約部分加群の和を M_0 とし, $M\neq M_0$ とする. すると仮定より, $M=M_0\oplus N$ を満たす部分加群 $N\neq O$ が存在する. このとき, 補題 5.3.7 より, N は既約加群 N_1 を含むが, このことは, M_0 の定義に反する. よって, $M=M_0$ でなければならない. □

系 5.3.10 M を完全可約加群とする. このとき, M の部分加群や剰余加群は, 再び, 完全可約である.

証明　N を M の部分加群とする. L を N の部分加群とし, $M=L\oplus M'$ とする. このとき, $N=L\oplus(N\cap M')$ が成り立つ. 従って, 定理 5.3.8 より, N は完全可約である.

また, $M=N\oplus M'$ と表すと, $M'\simeq M/N$. 従って, M/N は完全可約である. □

系 5.3.11 完全可約加群 M が極大条件と極小条件を共に満たすならば, M は有限個の既約加群の直和として表される：

$$M=M_1\oplus\cdots\oplus M_l\quad(M_i\text{ は既約}).$$

このとき, $\{M_1,\cdots,M_l\}$ は一意的に定まる.

証明　極大条件より, 極大部分加群 $M_1'\subset M$ が存在する. $M=M_1\oplus M_1'$ と表すと, M_1 は既約である. $M_1'\neq O$ ならば, 極大部分加群 $M_2'\subset M_1'$ が存在する. $M_1'=M_2'\oplus M_2$ と表すと, M_2 は既約である. M は極小条件を満たすので, この操作は有限回で止む. 従って, M は既約加群の直和で表される：

$$M=M_1\oplus\cdots\oplus M_l\quad(M_i\text{ は既約}).$$

このとき, $\{M_1,\cdots,M_l\}$ は, 組成剰余加群列なので, Jordan-H$\acute{\text{o}}$lder の定理により, 一意的に定まる. □

5.3.3 直既約加群と Krull-Remak-Schmidt の定理

M を O と異なる R-加群とする. M が非自明な部分加群の直和として表されないとき, M を **直既約加群** という.

命題 5.3.12 *M が極小条件を満たす加群ならば, M は有限個の直既約加群の直和として表される.*

証明 M の, 有限個の直既約部分加群の直和として表されない, O と異なる部分加群の集合を S とする. $S \neq \emptyset$ とすると, 極小条件から, 斯かる部分加群のうち極小となるもの M' が存在する. M' は O と異なり, 非自明な分解 $M' = M_1 \oplus M_2$ を持つ. このとき, $M_1, M_2 \notin S$ であり, M_1, M_2 は直既約加群の有限個の直和となる. これは, $M' \in S$ に反する. 従って, $S = \emptyset$ となり, 命題を得る. □

補題 5.3.13 *M を直既約 R-加群とし, $N \neq O$ を R-加群とする. 加群全射 $f : M \longrightarrow N$ に対し, 加群射 $h : N \longrightarrow M$ が存在し $f \circ h$ は N の R-同型射であるとする. このとき, f, h は共に同型射である.*

証明 $M = \mathrm{Ker}(f) \oplus h(N)$ が成り立ち, $h(N) \neq O$. 実際, 任意の $x \in M$ に対し, $y := x - (h \circ (f \circ h)^{-1})(f(x))$ とおく. すると, $f(y) = f(x) - f(x) = 0$ となり, $y \in \mathrm{Ker}(f)$. よって, $x = h((f \circ h)^{-1}(f(x)) + y \in h(N) + \mathrm{Ker}(f)$. また, $\mathrm{Ker}(f) \cap h(N) = O$ は容易にわかる. M は直既約なので, $\mathrm{Ker}(f) = O$ となり, f は同型射である. □

補題 5.3.14 *M を直既約 R-加群とし, $h_i \in \mathrm{End}_R(M)$ $(1 \leq i \leq n)$ とする. $h_1 + \cdots + h_n$ が M の R-同型射ならば, ある h_i は R-同型射となる.*

証明 $n = 2$ として良い. $f = h_1 + h_2$ とし, $g_i = h_i \circ f^{-1}$ $(i = 1, 2)$ とすると, $I = g_1 + g_2$. g_1, g_2 が共に冪零ならば, 即ち $g_1^{k_1} = 0, g_2^{k_2} = 0$ を満たす非負整数 k_1, k_2 が存在するならば, k を十分大きく取ると,

$$I = (g_1 + g_2)^k = \sum_{r=0}^{k} \binom{k}{r} g_1^r g_2^{k-r} = 0.$$

これは不合理で, g_1, g_2 の一方は冪零でない. $g := g_1$ が冪零でないとして良い.

さて, $N_j = \mathrm{Ker}(g^j)$ とすると,

$$N_1 \subset N_2 \subset \cdots ; \quad M \supset g(M) \supset g^2(M) \supset \cdots .$$

M は極大条件と極小条件を満たすので, ある t が存在して,

$$N_t = N_{t+1} + \cdots ; \quad g^t(M) \supset g^{t+1}(M) \supset \cdots .$$

g は冪零でないので, $0 \neq g^t \in \mathrm{End}_R(M)$. 加群全射 $g^t : M \longrightarrow N := g^t(M)$ と自然な単射 $\phi : N = g^t(M) \longrightarrow M$ を考える. そこで, $\psi := g^t \circ \phi$ とおき, $N = g^t M$ の任意の元 $g^t x$ を採る. $g^t(g^t x) = 0$ とすると, $x \in \mathrm{Ker}(g^{2t}) = N_{2t} = N_t$ となり, $g^t x = 0$. よって, ψ は単射である. また, 任意の $y = g^t x \in N = g^t M$ に対し, $g^{2t} M = g^t M$ なので, $y = g^{2t} z$ $(\exists z \in M)$. すると, $y = g^t(g^t z) \in g^t M$. 従って, ψ は全射である. よって, $\psi : g^t M \longrightarrow g^t M$ は同型射である. M は直既約なので, 補題 5.3.13 より, $g^t : M \longrightarrow N$ は同型射であり, 自然な単射 $g^t M \longrightarrow M$ も同型射である. g^t が同型射ならば, g も同型射である. □

定理 5.3.15（Krull-Remak-Scmidt の定理）M は極大条件と極小条件を満たす R-加群とする.

$$M = M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots \oplus N_s$$

を直既約加群への直和分解とする. このとき, $r = s$ であり, 適当に並べ替えると,

$$M_1 \simeq N_1, \cdots, M_r \simeq N_r$$

が成り立つ.

証明　r に関する帰納法で示す. $r = 1$ のとき, $s = 1$ であり, 定理は正しい. $r > 1$ とし, $r - 1$ まで定理は正しいとする. 射影を

$$p_i : M \longrightarrow M_i; \quad q_j : M \longrightarrow N_j$$

とすると,

$$I_M = p_1 + \cdots + p_r = q_1 + \cdots + q_s, \quad p_i p_j = q_i q_j = 0 \quad (i \neq j)$$

が成り立つ. よって,

$$p_1 = p_1 q_1 + \cdots + p_1 q_s.$$

$p_1 q_j|_{M_1}$ も同じ文字で表すことにすると,

$$p_i q_j : M_1 \longrightarrow M_1 \ (1 \leq j \leq s), \quad I_{M_1} = p_1 q_1 + \cdots + p_1 q_s.$$

すると, 補題 5.3.14 より,

$$M_1 \xrightarrow{q_1} N_1 \xrightarrow{p_1} M_1$$

が同型射として良い. よって, 補題 5.3.13 より, $q_1 : M_1 \longrightarrow N_1$ と $p_1 : N_1 \longrightarrow M_1$ は共に同型射である.

ここで, $N_1 + M_2 + \cdots + M_r$ が直和であることを示す. $y_1 + x_2 + \cdots + x_r = 0$ と仮定する. p_1 を施すと, $p_1(y_1) = 0$ であり, p_1 は同型射なので, $y_1 = 0$. すると, $x_2 = \cdots = x_r = 0$. さて,

$$M' = N_1 \oplus M_2 \oplus \cdots \oplus M_r$$

とし,

$$f = (q_1|_{M_1})p_1 + p_2 + \cdots + p_r : M \longrightarrow M$$

とする. このとき, $f : M \longrightarrow \mathrm{Im}(f) = M'$ は同型射であり, $f|_{M_1} : M_1 \longrightarrow N_1$ も同型射である.

$$M \supset fM \supset f^2 M \supset \cdots$$

であり, M は極小条件を満たすので, 非負整数 n が存在して

$$f^n M = f^{n+1} M = \cdots.$$

$x \in M$ に対し, $f^{n+1} x' = f^n x$ を満たす $x' \in M$ が存在する. このとき, $f^n(fx' - x) = 0$ であり, f は単射なので, $fx' = x$. 従って, $M = fM = M'$ を得る. よって, $f : M \longrightarrow M$ は同型射で, $f(M_1) = N_1$ を満たすので,

$$M_2 \oplus \cdots M_r \simeq M/M_1 \simeq M/N_1 \simeq N_2 \oplus \cdots \oplus N_s.$$

従って, 帰納法の仮定により, $r-1=s-1$ が成り立ち, 適当に並べ替えて, $M_i \simeq N_i$ $(2 \leq i \leq r)$. □

系 5.3.16 M は極大条件と極小条件を満たす R-加群とし, 直既約部分加群の直和とする：

$$M = M_1 \oplus \cdots \oplus M_r.$$

このとき, M の任意の直和因子 N に対し, $1 \leq i_1 < \cdots < i_k \leq r$ が存在して, $N \simeq M_{i_1} \oplus \cdots \oplus M_{i_k}$ となる.

証明 N は M の直和因子なので $M = N \oplus N'$ と表される. N, N' は極小条件を満たすので, 命題 5.3.12 により, 直既約加群の直和と表される：

$$N = N_1 \oplus \cdots \oplus N_k, \quad N' = N'_1 \oplus \cdots \oplus N'_{k'}.$$

すると, 定理より, 適当に並べ替えて,

$$N_1 \simeq M_{i_1}, \cdots, N_k \simeq M_{i_k}$$

を得る. □

第6章　加群 II

6.1　代数

6.1.1　定義と例

R を可換環とし, A を R-加群とする. A と R-双線形射 $\phi : A \times A \longrightarrow A$ の組 $(A;\phi)$ を, 通常, R-代数という. A 上の二項演算 ϕ が結合法則を満たすとき, (A,ϕ) は結合的代数と呼ばれる.

例 6.1.1 L を可換環 R 上の加群とする. L 上の双線形射

$$[\ ,\ ] : L \times L \longrightarrow L$$

が次を満たすとき, $(L;[\ ,\ ])$ を R 上の **Lie 代数** という：

(1) $[X,X] = 0 \quad (\forall X \in L)$,

(2) （Jacobi の恒等式）

$$[X,[Y,Z]] + [Z,[X,Y]] + [Y,[Z,X]] = 0 \quad (\forall X,Y,Z \in L).$$

例 6.1.2 $A, B \in \mathrm{M}_n(\mathbb{R})$ に対し,

$$[A,B] = AB - BA$$

と定める. このとき, $(\mathrm{M}_n(\mathbb{R}),[\ ,\ ])$ は $\mathbb{R}$ 上 n^2 次元の Lie 代数をなす. この Lie 代数を $\mathfrak{gl}_n(\mathbb{R})$ と表す.

可換環 R から環 A への環射 $f : R \longrightarrow A$ の像 $f(R)$ は A の中心に含まれるとする. 即ち,

$$f(x)a = af(x) \quad (\forall x \in R,\ \forall a \in A)$$

を満たすとする. このとき, A は

$$R \times A \longrightarrow A; \quad (x,a) \longmapsto x \cdot a = f(x)a$$

をスカラー倍とすることにより, R-加群となる. A における積

$$\times : A \times A \longrightarrow A$$

は, R-双線形射である. 実際,

$$(a+a')b = ab + a'b, \quad a(b+b') = ab + ab' \quad (\forall a,a',b,b' \in A),$$

$$(x \cdot a)b = f(x)ab = x \cdot (ab) = a(x \cdot b) \quad (\forall x \in R, \forall a,b \in A)$$

が成り立つ. $f : R \longrightarrow A$ を, または単に, A を R-**多元環**, または, R-**代数** という.

例 6.1.3 可換環 R の元を係数とする n 次正方行列全体のなす全行列環 $\mathrm{M}_n(R)$ に対し,

$$R \longrightarrow \mathrm{M}_n(R); \quad r \longmapsto rI_n$$

は, R-多元環である.

R を可換環とし, G を（乗法的）単位半群とする. G から R への写像 f に対し,

$$\mathrm{supp}(f) = \{x \in G \mid f(x) \neq 0\}$$

を f の台という. 台が有限集合となる G から R への写像の全体を $R[G]$ と表す. $f, g \in R[G]$ の和を

$$(f+g)(x) = f(x) + g(x) \quad (x \in G)$$

と定めることにより, $R[G]$ は加法群をなす. f, g の積を

$$(fg)(z) = \sum_{(x,y)\in G\times G; xy=z} f(x)g(y)$$

により定める. $\mathrm{supp}(f), \mathrm{supp}(g)$ が有限集合なので, 上の和は実質的に有限和となることに注意する.

$$\mathrm{supp}(fg) \subset \mathrm{supp}(f)\mathrm{supp}(g)$$

が成り立つので, $fg \in R[G]$.

補題 6.1.1 $(R[G]; +, \cdot)$ は環をなす.

証明　全ての $x \in G$ に対し, 0 を値にとる零写像が零元であり, $1(1_G) = 1_R, 1(x) = 0$ $(x \in G - \{1_G\})$ なる写像 1 が単位元である. 積に関する結合法則のみを証明し, 他は演習問題とする. $f, g, h \in R[G]$ と任意の $z \in G$ に対し,

$$\begin{aligned}
(f(gh))(z) &= \sum_{x,y;xy=z} f(x)(gh)(y) \\
&= \sum_{x,y;xy=z} f(x)\Big(\sum_{u,v;uv=y} g(u)h(v)\Big) \\
&= \sum_{x,y;xy=z} \Big(\sum_{u,v;uv=y} f(x)g(u)h(v)\Big) \\
&= \sum_{x,u,v;xuv=z} (f(x)g(u)h(v)).
\end{aligned}$$

同様にして,

$$((fg)h)(z) = \sum_{x,u,v;xuv=z} (f(x)g(u)h(v)).$$

従って, $f(gh) = (fg)h$ を得る. □

R の元 r に対し, $\iota(r)(1_G) = r, \iota(r)(x) = 0$ $(\forall x \in G - \{1_G\})$ とすると, 環単射 $\iota : R \longrightarrow R[G]$ を得る. 更に, 任意の $f \in R[G]$ に対し,

$$(\iota(r)f)(x) = rf(x) = f(x)r = (f\iota(r))(x) \quad (\forall x \in G)$$

なので, $\iota(R)$ は, $R[G]$ の中心に含まれる. 従って, 次の定理を得る：

定理 6.1.2 $\iota : R \longrightarrow R[G]$ は R-代数である.

$f \in R[G]$ に対し, $f(x) = a_x$ と表し,

$$f = \sum_{x \in G} a_x x$$

と表すことにする. すると $1 = 1_G$ であり,

$$(\sum_{x \in G} a_x x) + (\sum_{x \in G} b_x x) = \sum_{x \in G} (a_x + b_x)x,$$

$$(\sum_{x \in G} a_x x)(\sum_{x \in G} b_x x) = \sum_{x,y \in G} (a_x b_y)xy.$$

G が群のとき, $R[G]$ を R 上の **群環** という.

例 6.1.4 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ とし, $(\mathbb{N}_0)^n$ は, 和を

$$(k_1, \cdots, k_n) + (l_1, \cdots, l_n) = (k_1 + l_1, \cdots, k_n + l_n)$$

と定めることにより, 単位半群をなす. $n = \infty$ でもよいことに注意する.

R を可換環とし, $X_1, \cdots, X_n$ を文字とする. $f \in R[(\mathbb{N}_0)^n]$ を

$$f = f(X_1, \cdots, X_n) = \sum_{(k_1, \cdots, k_n)} f(k_1, \cdots, k_n) X_1^{k_1} \cdots X_n^{k_n}$$

と表す. $R[(\mathbb{N}_0)^n]$ を $R[X_1, \cdots, X_n]$ と表し, R **上の** n **変数多項式環** という.

$f : R \longrightarrow A$ を可換環の環射とし, S を A の部分集合とする. $f(R) \cup S$ を含む最小の, A の, 部分環を $R[S]$ と表す. $A = R[S]$ のとき, S は R-多元環として, A を **生成する** という. さて, $x_1, \cdots, x_n \in S$ と, $(k_1, \cdots, k_n) \in (\mathbb{N}_0)^n$ に対し,

$$x_1^{k_1} \cdots x_n^{k_n} \in A$$

を S の元からなる単項式という. S の元からなる単項式全体の集合を $M(S)$ と表す. A の部分集合 $M(S)$ が R 上一次独立のとき, S は, R 上 **代数的独立** という.

例 6.1.5 R を可換環とし, $S = \{X_1, \cdots, X_n\}$ を文字の集合とする. このとき, R 上の多項式環 $R[X_1, \cdots, X_n]$ の部分集合 S は, R 上代数的に独立である. また, S は R-多元環として, $R[X_1, \cdots, X_n]$ を生成する.

環射の重要な例の一つは, 多項式の変数に値を代入するものである.

補題 6.1.3 $f_0 : R \longrightarrow A$ を可換環の射とする. $S \subset A$ は, R 上代数的に独立で, $A = R[S]$ を満たすとする. 可換環の射 $f : R \longrightarrow B$ と写像 $\phi : S \longrightarrow B$ に対し, 環射

$$\Phi : A = R[S] \longrightarrow B$$

で

$$\Phi \circ f_0 = f, \quad \Phi(x) = \phi(x) \quad (\forall x \in S)$$

を満たすものが唯一つ存在する.

証明　$n=1$ の場合を示せば, 帰納法により結論を得る. $X=X_1, \alpha=\alpha_1$ と表す. 各多項式

$$f(X)=x_nX^n+\cdots+x_1X+x_0\in R[X]$$

に対し,

$$\Phi(f(X))=\phi(x_n)\alpha^n+\cdots+\phi(x_1)\alpha+\phi(x_0)$$

と定める.

$$f(X)=\sum_{k=0}^{n}x_kX^k,\quad g(X)=\sum_{l=0}^{m}y_lX^l\quad N=\max\{n,m\}$$

とする. 但し,

$$x_p=0,\ y_q=0\quad (n+1\le p\le N,\ m+1\le q\le N)$$

とする. このとき,

$$\Phi(f(X)+g(X))=\sum_{i=0}^{N}\phi(x_i+y_i)\alpha^i=\Phi(f(X))+\Phi(g(X)),$$

$$\Phi(f(X)g(X))=\Phi(\sum_{i=0}^{nm}(\sum_{j=0}^{i}x_jy_{i-j})X^i)=\sum_{i=0}^{nm}(\sum_{j=0}^{i}\phi(x_jy_{i-j}))\alpha^i=\Phi(f(X))\Phi(g(X)).$$

また, $\Phi(1)=\phi(1)=1$. 従って Φ は環射であり, $\Phi(X)=\alpha$ を満たす. 一意性は明らかであろう. □

単位半群 $(\mathbb{N}_0)^n$ は特別な性質を持つ. 即ち, 任意の $x\in(\mathbb{N}_0)^n$ に対し,

$$\{(x,y)\in(\mathbb{N}_0)^n\times(\mathbb{N}_0)^n\mid xy=z\}$$

は有限集合である.

$(\mathbb{N}_0)^n$ から可換環 R への写像の集合を $R[[(\mathbb{N}_0)^n]]$ と表す. $f,g\in R[[(\mathbb{N}_0)^n]]$ に対し, 和と積を

$$(f+g)(k_1,\cdots,k_n)=f(k_1,\cdots,k_n)+g(k_1,\cdots,k_n),$$

$$(fg)(k_1,\cdots,k_n)=\sum_{0\le l_1\le k_1,\cdots,0\le l_n\le k_n}f(l_1,\cdots,l_n))g(k_1-l_1,\cdots,k_n-l_n)$$

により定める. このとき, $R[[(\mathbb{N}_0)^n,R)]]$ は R-多元環をなす.

$X_1,\cdots,X_n$ を文字とするとき, 写像 $f\in R[[(\mathbb{N}_0)^n,R)]]$ と, 形式的和

$$f(X_1,\cdots,X_n)=\sum_{(e_1,\cdots,e_n)\in(\mathbb{N}_0)^n}f(e_1,\cdots,e_n)X_1^{e_1}\cdots X_n^{e_n}$$

を同一視する. $f(X_1,\cdots,X_n)$ を f に付随する R **係数** n **変数形式的冪級数** という. これら形式的冪級数の全体を $R[[X_1,\cdots,X_n]]$ と表し, R **係数** n **変数形式的冪級数環** という.

6.1.2 テンソル代数

V を体 K 上の n 次元線形空間とする. V の r 個のテンソル積 $T^r(V)$ の無限個の直和を

$$\mathbb{T}(V) = \oplus_{r=0}^{\infty} T^r(V) \quad (T^0(V) = K, T^1(V) = V)$$

と表す. 即ち, 有限個のテンソルの K 上の一次結合

$$\sum a_r \tau_r \quad (\tau_r \in T^r(V))$$

全体のなす（無限次元）線形空間を $T(V)$ と表す.

二つのテンソル

$$t_r = x_1 \otimes \cdots \otimes x_r \in T^r(V), \quad t_s = y_1 \otimes \cdots \otimes y_s \in T^s(V)$$

に対し, その積を

$$t_r \cdot t_s = x_1 \otimes \cdots \otimes x_r \otimes y_1 \otimes \cdots \otimes y_s \in T^{r+s}(V)$$

と定めることにより, $(T(V); +, \cdot)$ は環をなす. 更に, 環単射

$$\iota : K \longrightarrow T(V); \quad c \longmapsto c \in K = T^0 \subset T(V)$$

により, $T(V)$ は, K 上の線形空間をなしている：即ち, $t \in T(V)$ の $c \in K$ 倍が, $c \cdot t = \iota(c)t$ で定められている. 環 $T(V)$ と環単射 ι の組 $(T(V), \iota)$ は, K 上の代数である.

線形射 $\tau : V \longrightarrow T(V)$ を, $\tau(v) = v$ により定め, 組 $(T(V), \tau)$ を, V の **テンソル代数** という.

を V の **テンソル代数** という.

定理 6.1.4 （テンソル代数の普遍性）K 上の代数 $A = (A, \iota_A)$ と線形射 $\alpha : V \longrightarrow A$ の組 (A, α) に対し, $\alpha_* \circ \tau = \alpha$ を満たす代数射 $\alpha_* : T(V) \longrightarrow A$ が唯一つ存在する.

$(T(V), \tau)$ は, 同型を除いて, この性質を持つ唯一の組である.

証明 $(x_1, \cdots, x_r)$ に対し, $\alpha(x_1) \cdots \alpha(x_r)$ を対応させる写像は, α が線形射であり, A が代数なので, 多重線形射 $V^r = V \times \cdots \times V \longrightarrow A$ である. 従って, テンソルの普遍性により,

$$\alpha_*(x_1 \otimes \cdots \otimes x_r) = \alpha(x_1) \cdots \alpha(x_r)$$

を満たす線形射 $\alpha_* : T^r(V) \longrightarrow A$ が一意的に存在する. よって, $\alpha_*(c) = \iota_A(c)$ $(c \in K)$ とすることにより, 線形射 $\alpha_* : T(V) \longrightarrow A$ を得る.

$$\alpha_* \left((x_1 \otimes \cdots \otimes x_r)(y_1 \otimes \cdots \otimes y_s)\right) \\ = \alpha(x_1) \otimes \cdots \otimes \alpha(x_r)\alpha(y_1) \otimes \cdots \otimes \alpha(y_s)$$

なので, α_* は代数射である. 一意性は明らかである.

普遍性より, 定理 **??** と同様にして, 後半が示される. □

r 次対称群 S_r は, 次のようにして, テンソル空間 $T^r(V)$ に作用する：

$\sigma \in S_n$ とする. このとき,

$$V^r \longrightarrow T^r(V) \quad (x_1, \cdots x_r) \longmapsto x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}$$

は多重線形射である. 従って, テンソル積の普遍性により, 線形射

$$P_\sigma : T^r(V) \longrightarrow T^r(V) \quad (x_1 \otimes \cdots \otimes x_r) = x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}$$

が存在する. このとき,

$$\begin{aligned} P_\sigma P_\tau(x_1 \otimes \cdots \otimes x_r) &= P_\sigma(x_{\tau(1)} \otimes \cdots \otimes x_{\tau(r)} \\ &= x_{\sigma(\tau(1))} \otimes \cdots \otimes x_{\sigma(\tau(r))} \\ &= P_{\sigma\tau}(x_1 \otimes \cdots \otimes x_r) \end{aligned}$$

が成り立ち,

$$P_{\sigma\tau} = P_\sigma P_\tau$$

を得る.

定義 6.1.5 $t_r \in T^r(V)$ が

$$P_\sigma(t_r) = \begin{cases} t_r & \\ \mathrm{sign}(\sigma) t_r & (\forall \sigma \in S_r) \end{cases}$$

を満たすとき, t_r を, それぞれ, **対称テンソル**, **歪対称テンソル** という.

また, 任意の互換 τ に対し,

$$P_\tau(t_r) = 0$$

を満たす t_r を **交代テンソル** という.

問 6.1.6 交代テンソルは, 歪対称テンソルであることを示せ. また, K の標数が 2 でない, 即ち, $1 + 1 \neq 0$ ならば, 歪対称テンソルは交代テンソルであることを示せ.

6.1.3　対称代数と外積代数

W を体 K 上の n 次元空間とし, $(f^1, \cdots, f^n)$ を基底とする. $I = \{1, \cdots, n\}$ とし, I の部分集合 S に対し, 記号 f^S を定める. 但し, $f^\emptyset = 1$ と表す. $\{f^S \mid S \subset I\}$ を基底とする 2^n 次元線形空間を $\Lambda.W$ と表す. すると, $\Lambda.W$ は, 部分空間

$$\Lambda_r(W) = \langle f^S \mid |S| = r \rangle$$

の直和と表される：

$$\Lambda.W = \Lambda_0(W) \oplus \Lambda_1 W \oplus \Lambda_2(W) \oplus \cdots \oplus \Lambda_n W.$$

例 6.1.6 $1 = f^\emptyset$ と体 K の単位元 1, $f^{\{i\}}$ と f^i を同一視して,

$$\Lambda_0 W = K, \quad \Lambda_1 W = W.$$

$S,T \subset I$ に対し,

$$k(S,T) = \{(i,j) \mid i \in S, j \in T, i > j\}$$

と定め,

$$\epsilon(S,T) = \begin{cases} (-1)^{|k(S,T)|} & S \cap T = \emptyset \\ 0 & S \cap T \neq \emptyset \end{cases}$$

と定める. そこで,

$$f^S \wedge f^T = \epsilon(S,T) f^{S \cup T}$$

と定義すると, 線形性により, $\Lambda.W$ の二項演算 $\wedge$ が定まり, $(\Lambda.W; +, \wedge)$ は環をなす. $\Lambda.W$ と環単射 $\iota : K \longrightarrow \Lambda.W$ の組 $(\Lambda.W, \iota)$ は K 上の代数である.

例 6.1.7

$$1 \wedge e^S = e^S \quad (\forall S \subset I),$$
$$f^i \wedge f^i = 0, \quad f^j \wedge f^i = -f^i \wedge f^j \ (i \neq j).$$

例題 6.1.7 $R,S,T \subset I$ に対し,

$$(f^R \wedge f^S) \wedge f^T = f^R \wedge (f^S \wedge f^T)$$

を確かめよ.

（解） R,S,T のいずれか二つが, 交われば, 両辺が 0 となり等しい. そこで, これらは互いに交わらないとする. このとき,

$$k(R \cup S, T) = k(R,T) + k(S,T), \quad k(R, S \cup T) = k(R,S) + k(R,T)$$

と直和になることに注意する. すると,

$$\begin{aligned} (f^R \wedge f^S) \wedge f^T &= \epsilon(R,S) f^{R \cup S} f^T \\ &= \epsilon(R,S)\epsilon(R \cup S, T) f^{R \cup S \cup T} \\ &= (-1)^{|k(R,S|+|k(R,T)|+|k(S,T)|} f^{R \cup S \cup T} \\ &= f^R \wedge (f^S \wedge f^T) \end{aligned}$$

を得る. □

例 6.1.8 $i_1 < \cdots < i_r$ のとき, $S = \{i_1, \cdots, i_r\}$ とすれば

$$f^{i_1} \wedge \cdots \wedge f^{i_r} = f^S.$$

f^i に $f^{\{i\}} (= f^i)$ を対応させることにより, 線形射

$$\lambda : W \longrightarrow \Lambda.W$$

を得る. λ は,

$$\lambda(w) \wedge \lambda(w) = 0 \quad (\forall w \in W)$$

を満たす. 代数 $\Lambda.W$ と λ の組 $(\Lambda.W, \lambda)$ を, W の **外積代数** という.

次の普遍性は, 定理 6.1.4 と同様にして示される.

定理 6.1.8（外積代数の普遍性）K 上の代数 A と, $\alpha(w)^2 = 0$ $(\forall w \in W)$ を満たす線形射 $\alpha : W \longrightarrow A$ の組 (A, α) に対し, $\alpha_* \circ \lambda = \alpha$ を満たす代数射 $\alpha_* : \Lambda.(W) \longrightarrow A$ が唯一つ存在する.

$(\Lambda.W, \lambda)$ は, 同型を除いて, この性質を持つ唯一の組である.

問 6.1.9 定理を証明せよ.

問 6.1.10 $\xi \in \Lambda_k W, \eta \in \Lambda_l W$ に対し,

$$\xi \wedge \eta = (-1)^{kl} \eta \wedge \xi$$

が成り立つことを示せ.

p-ベクトルのなす部分空間 $\Lambda_p W$ の普遍性を考察する.

$$\wedge_p : W^p \longrightarrow \Lambda_p W; \quad (\xi^1, \cdots, \xi^p) \longmapsto \xi^1 \wedge \cdots \wedge \xi^p$$

は交代多重線形射である. 即ち, 多重線形射であり,

$$\xi^1 \wedge \cdots \wedge \xi^p = 0 \quad (\xi^i = \xi^j \ (i \neq j)$$

を満たす. このとき, 組 $(\Lambda_p W, \wedge_p)$ は, 次の普遍性を持つ. その証明は, 行列式の特徴付けの証明の類似である：

定理 6.1.11（p-ベクトル空間の普遍性）$D : W^r \longrightarrow U$ を交代多重線形射とするとき, $D_* \circ \wedge_p = D$ を満たす線形射 $D_* : \Lambda_p W \longrightarrow U$ が一意的に存在する.

$(\Lambda_p W, \wedge_p)$ は, 同型を除いて, この性質を持つ唯一の組である.

証明　$D_*(f^S) = D(f^{i_1}, \cdots, f^{i_p})$ により, 線形射 $D_* : \Lambda_p W \longrightarrow U$ を定める. すると,

$$\xi^i = \sum_{j=1}^{n} a^i_j f^j \quad (1 \leq i \leq p)$$

に対し,

$$\begin{aligned} D_*(\xi^1 \wedge \cdots, \wedge \xi^p) &= (\sum_j a^j_1 f^j) \wedge \cdots (\sum_j a^j_p f^j) \\ &= \sum_{j_1, \cdots, j_p} a_{1j_1} \cdots a_{pj_p} f^{j_1} \wedge \cdots f^{j_n} \\ &= \sum_{j_1, \cdots, j_p, \neq} a_{1j_1} \cdots a_{pj_p} f^{j_1} \wedge \cdots f^{j_p} \end{aligned}$$

を得る. ここで, $S = \{j_1, \cdots, j_p\} = \{i_1 < \cdots < i_p\}$ とすれば,

$$\begin{aligned} D_S &:= \det \begin{pmatrix} a^1_{i_1} & \cdots & a^1_{i_p} \\ \vdots & & \vdots \\ a^p_{i_1} & \cdots & a^p_{i_p} \end{pmatrix} \\ &= \sum_{S=\{j_1, \cdots, j_p\}} \operatorname{sign} \begin{pmatrix} i_1 & \cdots & i_p \\ j_1 & \cdots & j_p \end{pmatrix} a_{1j_1} \cdots a_{pj_p} \end{aligned}$$

を得る. 従って,

$$D_*(\xi^1 \wedge \cdots, \wedge\xi^p) = \sum_S D_S f_S.$$

同様にして,

$$D(\xi^1, \cdots, \xi^p) = \sum_S D_S D(f^{i_1}, \cdots, f^{i_p})$$

を得る. よって, $D_* : \Lambda_p W \longrightarrow U$ が成り立つ.

一意性は明らかであり, 後半の証明は, いつもの通り. □

線形射 $\phi : W \longrightarrow W'$ に対し, $\Lambda.W'$ において, $\phi(w) \wedge \phi(w) = 0$ $(\forall w \in W)$ が成り立つ. 従って, 外積代数 $\Lambda.W$ の普遍性により, 代数射

$$\Lambda.\phi : \Lambda.W \longrightarrow \Lambda.W'; \quad w_1 \wedge \cdots \wedge w_k \longmapsto \phi(w_1) \wedge \cdots \wedge \phi(w_k)$$

を得る. $\Lambda.\phi$ の $\Lambda_k W$ への制限は, 線形射

$$\Lambda_k\phi : \Lambda_k W \longrightarrow \Lambda_k W'$$

を得る.

例題 6.1.12 $\phi : W \longrightarrow W$ を線形射とする. このとき,

$$(\Lambda_n\phi) f^I = \det(\phi) f^I$$

が成り立つことを示せ.

（解） 線形射 ϕ の基底 (f^i) に関する表現行列を $A = (a_i^j)$ とする：$\phi(f^i) = A(f^i)$. このとき,

$$\begin{aligned}
(\Lambda.\phi)(f^I) &= \phi(f^1) \wedge \cdots \wedge \phi(f^n) \\
&= (\sum_j a_1^j f^j) \wedge \cdots (\sum_j a_n^j f^j) \\
&= \sum_{j_1, \cdots, j_n} a_{1j_1} \cdots a_{nj_n} f^{j_1} \wedge \cdots f^{j_n} \\
&= \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)} f^{\sigma(1)} \wedge \cdots f^{\sigma(n)}
\end{aligned}$$

を得る. 置換の符号と互換の関係を考慮して,

$$f^{\sigma(1)} \wedge \cdots f^{\sigma(n)} = \mathrm{sign}(\sigma) f^1 \wedge \cdots f^n.$$

従って, 行列式の完全展開より, 結論を得る. □

6.2 線形代数への応用

この節では, K を体とし, K 係数 n 次元縦数ベクトル全体のなす K 上の線形空間を K^n で表す. K 係数一変数多項式環 $K[X]$ 上の加群いくつかの直和の元も縦ベクトルで表す.

6.2.1　$K[X]$-加群 V

V を体 K 上の n 次元線形空間とし, $T : V \longrightarrow V$ を線形写像とする.
多項式

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$$

に対し,

$$f(T) := a_n T^n + \cdots + a_1 T + a_0 I \in \mathrm{End}_K(V)$$

と定める. すると,

$$K[X] \times V \longrightarrow V; \quad (f(X), v) \longmapsto f(X) \cdot v = f(T)v$$

が定まり, V は $K[X]$-加群となる.

注意 6.2.1 体 K は $K[X]$ の部分環と見なせる. すると $K[X]$-加群 V は K-加群, 即ち, K 上の線形空間と見なせる. これは K 上のベクトル空間 V に他ならない. また

$$V \longrightarrow V, \quad v \longmapsto X \cdot v = Tv$$

は, K 上の線形写像である.

$\mathcal{B} = (v_1, \cdots, v_n)$ を K 上の線形空間 V の（順序付き）基底とし, $\mathcal{B}$ に関する T の表現行列を A とすると,

$$T(v_1, \cdots, v_n) = (v_1, \cdots, v_n)A.$$

$f(X) \in K[X]$ に対し,

$$f(A) = a_n A^n + \cdots + a_1 A + a_0 I$$

と定める.
n 個の多項式

$$h_i(X) = h_{i0} + h_{i1} X + \cdots + h_{iL} X^L \quad (h_{il} \in K,\ 1 \leq i \leq n,\ 0 \leq l \leq L)$$

を成分とする縦ベクトル $H(X) \in K[X]^n$ は,

$$H(X) = H_0 + XH_1 + \cdots + X^L H_L \quad (H_i \in K^n\ ; 1 \leq i \leq L),$$

$$H_l = {}^t(h_{1l}, \cdots, h_{nl}) \quad (1 \leq l \leq L)$$

と表わされる. $H(X) \neq 0$ のとき, $H(X)$ の次数を, $\max\{l \mid H_l \neq 0\}$ により定義する.
更に,

$$H(A) = H_0 + AH_1 + \cdots + A^L H_L \in K^n$$

と定める.
写像

$$\eta : K[X]^n \longrightarrow V, \quad H(X) \longmapsto h_1(X) \cdot v_1 + \cdots + h_n(X) \cdot v_n$$

は, $K[X]$-線形写像であり,

$$\begin{aligned}\eta(H) &= (h_{10}I + h_{11}T + \cdots + h_{1L}T^L)v_1 + \cdots + (h_{n0}I + h_{n1}T + \cdots + h_{nL}T^L)v_n \\ &= (v_1, \cdots, v_n)H_0 + T(v_1, \cdots, v_n)H_1 + \cdots + T^L(v_1, \cdots, v_n)H_L \\ &= (v_1, \cdots, v_n)(H_0 + AH_1 + \cdots + A^L H_L) \\ &= (v_1, \cdots, v_n)H(A)\end{aligned}$$

を満たす. 従って, 次を得る:

補題 6.2.1 $K[X]$-線形写像

$$\eta : K[X]^n \longrightarrow V, \quad H \longmapsto (v_1, \cdots, v_n)H(A)$$

は全射であり, $K[X]$-加群として,

$$K[X]^n/\mathrm{Ker}(\eta) \simeq V.$$

$K[X]^n$ は, $\mathrm{M}_n(K[X])$-加群と見なすと, 次を得る:

補題 6.2.2 $A \in \mathrm{M}_n(K)$ とする. 各 $H(X) \in K[X]^n$ は,

$$H(X) = (X \cdot I_n - A)Q(X) + H(A) \quad (\exists Q(X) \in K[X]^n)$$

と表される.

証明 $H(X) = 0$ のときは, 自明であり, $H(X)$ の次数が 0 のとき, $Q(X) = 0$ とすれば良い. $H(X)$ の次数が L 以下のとき正しいとし, $H(X)$ の次数が $L+1$ とする.

$$(X \cdot I_n - A)X^L H_{L+1} = X^{L+1}H_{L+1} - A(X^L H_{L+1})$$

なので, $G(X) := H(X) - (X \cdot I_n - A)X^L H_{L+1}$ の次数は, L 以下である. $G(A) = H(A) - (A^{L+1}H_{L+1} - A(A^L H_{L+1})) = H(A)$ なので, 帰納法の仮定により,

$$G(X) = H(X) - (X \cdot I_n - A)X^L H_{L+1} = (X \cdot I_n - A)Q(X) + H(A)$$

を満たす $Q(X)$ が存在し,

$$H(X) = (X \cdot I_n - A)X^L H_{L+1} + (X \cdot I_n - A)Q(X) + H(A) = (X \cdot I_n - A)(X^L H_{L+1} + Q(X)) + H(A).$$

よって, 帰納法により, 補題を得る. □

補題 6.2.3 $K[X]$-線形写像

$$\xi : K[X]^n \longrightarrow K[X]^n, \quad \xi(G) = (X \cdot I_n - A)G$$

に対し,

$$\mathrm{Im}(\xi) = \mathrm{Ker}(\eta).$$

証明　$G(X) \in K[X]^n$ を

$$G(X) = G_0 + XG_1 + \cdots + X^N G_N \quad (G_i \in K^n\ ; 1 \leq i \leq N)$$

と表すとき,

$$\begin{aligned} (6.1) \qquad \xi(G)(X); &= \xi(G(X)) = (XI_n - A)G \\ &= -AG_0 + X(G_0 - AG_1) + \cdots + X^n(G_{N-1} - AG_N) + X^{N+1}G_N \end{aligned}$$

なので, $\xi(G)(A) = 0$. 従って, η の定義より, $\eta(\xi(G)) = (v_1, \cdots, v_n)0 = 0$. よって, $\mathrm{Im}(\xi) \subseteq \mathrm{Ker}(\eta)$.

逆を示す. $H(X) \in K[X]^n$ が $\eta(H(X)) = (v_1, \cdots, v_n)H(A) = 0$ を満たすとする. このとき, $H(A) = 0$ であり, 前補題により,

$$H(X) = (X \cdot I - A)Q(X) \quad (Q(X) \in K[X]^n)$$

と表される. 従って, $\xi(Q(X)) = H(X)$. □

有限生成 $K[X]$-加群 V に対し, 基本定理 **??** は次のように述べられる.

定理 6.2.4 体 K 上のベクトル空間 V から V への線形写像 $T : V \longrightarrow V$ の（或る基底に関する）表現行列を A とする. このとき, 最高次係数が 1 の多項式 $d_i(X)$ で, 次を満たすものが一意的に存在する：

(1) $d_1(X) | \cdots | d_r(X)$.

(2) 行列 $X \cdot I_n - A$ は

$$(6.2) \qquad \begin{pmatrix} I_{n-r} & 0 & \cdots & 0 \\ 0 & d_1(X) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r(X) \end{pmatrix}$$

に対等である.

(3) $K[X]$-加群として

$$(6.3) \qquad V \simeq K[X]/(d_1(X)) \oplus \cdots \oplus K[X]/(d_r(X)).$$

特に, T の特性多項式 $P_T(X)$ は,

$$P_T(X) = d_1(X) \cdots d_r(X).$$

$d_1(X), \cdots, d_(X)$ を T の **単因子** という.

6.2.2 最小多項式と Cayley-Hamilton の定理

V を体 K 上の n 次元線形空間とし, $T : V \longrightarrow V$ を線形写像とする.

定義 6.2.5 環射

$$\phi : K[X] \longrightarrow \mathrm{End}_K(V), \quad \phi(X) = T$$

の核は, 単項イデアルであり, その生成元を, T の **最小多項式** という. 即ち, $f(T) = O$ となる次数最小の 0 と異なる多項式を T の **最小多項式** という. 以下, 最小多項式の最高次係数は 1 とする.

最高次係数が 1 の $k(\geq 1)$ 次の多項式

$$d(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0$$

に対し, $K[X]$-加群

$$V_d := K[X]/(d(X))$$

を調べよう.

$X^{k-1}, \cdots, X, 1$ を含む剰余類をそれぞれ $[X^{k-1}], \cdots, [X], [1]$ と表す. すると

$$\mathcal{B}_d := ([X^{k-1}], \cdots, [X], [1])$$

は $K[X]/(d(X))$ の K 上の基底をなし, $\dim_K(K[X]/(d(X))) = k$ である. スカラー倍

$$T_X : K[X]/(d(X)) \longrightarrow K[X]/(d(X)), \quad v \longmapsto Xv \tag{6.4}$$

は K-線形写像であり, $\mathcal{B}_d$ に関する表現行列は

$$M_d = \begin{pmatrix} -a_{k-1} & 1 & 0 & \cdots & 0 & 0 \\ -a_{k-2} & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ -a_1 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \in \mathrm{M}_k(K). \tag{6.5}$$

即ち,

$$T_X\mathcal{B}_d = \mathcal{B}_dM_d \tag{6.6}$$

が成り立つ.

補題 6.2.6 行列 $XI_k - M_d \in \mathrm{M}_k(K[X])$ と

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & d(X) \end{pmatrix}$$

は対等である. 特に, T_X の固有多項式は $d(X)$ である.

問 6.2.7 上の補題を示せ.

補題 6.2.8 最高次係数が 1 で, 次数が 1 以上の多項式 $d(X) \in K[X]$ に対し, 線形写像

$$T_X : K[X]/(d(X)) \longrightarrow K[X]/(d(X)), \quad v \longmapsto X \cdot v$$

の最小多項式は $d(X)$ である.

証明 $f(X)$ を最小多項式とする. $f(T_X)[1] = f(X) \cdot [1] = [f(X)] = [0]$ なので, $f(X) \in (d(X))$ であり, f は d の倍数. また, $0 \leq r \leq \deg(d) - 1$ に対し, $d(T_X)[X^r] = d(X) \cdot [X^r] = [d(X)X^r] = [0]$ なので, $\mathrm{End}_K(K[X]/(d(X)))$ の元として $d(T_X) = 0$. 従って, 最小多項式の定義より, $f|d$. よって, $f = d$. □

定理 6.2.9 線形写像 $T : V \longrightarrow V$ の単因子を $d_1(X), \cdots, d_r(X)$ とすれば,

(1) $d_r(X)$ は, T の最小多項式である.

(2) $P_T(X) = d_1(X) \cdots d_r(X)$.

(3) (Cayley-Hamilton) $P_T(T) = O$.

証明 (1) は, 補題 6.2.8 から, 直ちに得られる. (2) は, 定理 6.2.4 で示されている. (3) は, (1) から得られる. □

系 6.2.10 $T : V \longrightarrow V$ を 体 K 上の n 次元線形空間 V から V への線形写像とする. このとき, T の固有多項式の根の集合と, T の最小多項式の根の集合は一致する.

証明 単因子の定義より, $d_i | d_{i+1}$ が成り立つので, 定理 6.2.9 (2) より結論を得る. □

例 6.2.1 $a_1, \cdots, a_r$ を互いに異なる K の元とする. このとき対角行列

$$a_1 I_{k_1} \oplus \cdots \oplus a_r I_{k_r}$$

の最小多項式は

$$(X - a_1) \cdots (X - a_r)$$

である.

例 6.2.2

$$\mathcal{B} = ([X^{t-1}], \cdots, [T], [1])$$

は, K 上 t 次元線形空間 $K[X]/(X^t)$ の, 基底をなす. 線形写像

$$T : K[X]/(X^t) \longrightarrow K[X]/(X^t); \quad [f(X)] \longmapsto X[f(X)] = [Xf(X)]$$

の, $\mathcal{B}$ に関する表現行列は次の通り：

$$T\mathcal{B} = \mathcal{B}N, \quad N = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

行列 $XI_t - N$ と

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & X^t \end{pmatrix}$$

は対等である.

ϕ の特性多項式と最小多項式は, 共に, X^t に等しい.

正方行列 B は,

$$B^k = O \quad (\exists k \in \mathbb{N})$$

を満たすとき, **冪零行列** と呼ばれる. 上に述べた N は, その例である.

問 6.2.11 行列

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

の最小多項式を求めよ.

6.2.3 Jordan 標準形

この小節では, $K[X]$-加群 V を更に細かく分解することを考える.

補題 6.2.12 多項式 $d(X)$ が

$$d(X) = (X - \alpha_1)^{e_1} \times \cdots \times (X - \alpha_t)^{e_t}, \quad \alpha_i \in K, \alpha_i \neq \alpha_j \ (i \neq j)$$

と因数分解されるならば, $K[X]$-加群として,

$$K[X]/(d(X)) \simeq K[X]/(X - \alpha_1)^{e_1} \oplus \cdots \oplus K[X]/(X - \alpha_t)^{e_t}.$$

証明 中国剰余定理から直ちに得られる. □

$K[X]$-加群 $K[X]/((X - \alpha)^e)$ $(\alpha \in K)$ を自然に K 上のベクトル空間と見るとき

$$\mathcal{B} = ([(X - \alpha)^{e-1}], \cdots, [X - \alpha], [1])$$

は基底である. K 上の線形写像

$$T := T_X : K[X]/((X-\alpha)^e) \longrightarrow K[X]/((X-\alpha)^e), \quad [F(X)] \mapsto X \cdot [F(X)] = [XF(X)]$$

を考える.

$$X[(X-\alpha)^k] = [(X-\alpha)^{k+1}] - \alpha[(X-\alpha)^k]$$

となるので, この線形写像の基底 $\mathcal{B}$ に関する表現行列は次のようになる.

$$X \cdot \mathcal{B} = \mathcal{B}J(\alpha, e), \quad J(\alpha, e) = \begin{pmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \alpha & 1 \\ & & & & \alpha \end{pmatrix} \in \mathrm{M}_e(K).$$

ここで, 空白部は 0 を表す.

行列 $J(\alpha, e)$ を α に関する e 次の **ジョルダン細胞** という.

例 6.2.3

$$J(\alpha, 1) = (\alpha), \;\; J(\alpha, 2) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}, \;\; J(\alpha, 3) = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}.$$

ジョルダン細胞を幾つか対角線上に並べた行列

$$\begin{pmatrix} J(\alpha_1, n_1) & O & \cdots & O \\ O & J(\alpha_2, n_2) & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & J(\alpha_s, n_s) \end{pmatrix} = J(\alpha_1, n_1) \oplus J(\alpha_2, n_2) \oplus \cdots \oplus J(\alpha_s, n_s)$$

を **ジョルダン行列** という.

定理-定義 6.2.13 V を体 K 上の n 次元線形空間とし, $f : V \rangle V$ を K 上の線形写像とする. f の固有値は全て K に含まれるとする. このとき V の基底 $\mathcal{B}$ が存在し, f の $\mathcal{B}$ に関する表現行列が次のようになる:

$$J(f) = J(\alpha_1, d_1) \oplus J(\alpha_2, d_2) \oplus \cdots \oplus J(\alpha_s, d_s).$$

$J(f)$ を f の **ジョルダン標準形** という. f のジョルダン標準形は細胞の並べ替えを除いて一意的に定まる.

証明　一意性以外は, 定理 6.2.4, 補題 6.2.12 と, それに続く議論から得られる. また, 一意性は, 定理 **??** により得られる. □

定理を行列の場合に書換えて次を得る.

定理-定義 6.2.14 行列 $M \in \mathrm{M}_n(K)$ の固有値が根が全て K に含まれるならば, M はジョルダン行列 $J(M)$ に相似である, 即ち $J(M) = P^{-1}MP$ となる正則行列 $P \in \mathrm{GL}_n(K)$ が存在する. $J(M)$ を M の **ジョルダン標準形** という. また, $N \in \mathrm{M}_n(K)$ が M と相似である為の必要十分条件は $J(M)$ と $J(N)$ が, ジョルダン細胞の順序を除いて, 一致することである.

代数学の基本定理より, 複素数係数多項式は, 一次式の積に因数分解される. 従って, 次を得る.

系 6.2.15 複素数行列 $M \in \mathrm{M}_n(\mathbb{C})$ は, ジョルダン行列に相似である.

系 6.2.16 行列 $M \in \mathrm{M}_n(K)$ に対し, $P^{-1}MP$ がジョルダン行列となる正則行列 $P \in \mathrm{GL}_n(K)$ が存在する為の必要十分条件は M の固有多項式の根が全て K に含まれることであるとなることである.

系 6.2.17 行列 $M \in \mathrm{M}_n(X)$ が, $\mathrm{M}_n(K)$ に於いて, 対角行列に相似である必要十分条件は, M の固有多項式の根は, 全て K に含まれ, M の最小多項式が重根を持たないことである.

証明 最小多項式が重根を持たなければ, M のジョルダン標準形は対角行列である. 逆に最小多項式が重根を持てば, ジョルダン細胞で対角行列とならないものが存在する. □

例 6.2.4 $M^m = I_n$ を満たす複素係数 n 次正方行列 M は, 対角行列に相似である.

行列 $M \in \mathrm{M}_n(\mathbb{C})$ の最小多項式, 固有多項式, ジョルダン標準形を求める手順は, 以下の通り. まず, 行列 $X \cdot I_n - M$ に対等な行列

$$\begin{pmatrix} I_{n-r} & 0 & \cdots & 0 \\ 0 & d_1(X) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r(X) \end{pmatrix}, \quad d_1|d_2|\cdots|d_r$$

を求める. 但し, $d_i(X)$ は最高次係数が 1 の多項式. 次に, $d_i(X)$ を素因数分解する:

$$d_i(X) = \prod_{j=1}^{l_i} (X - \alpha_{ij})^{e_{ij}}, \quad 1 \leq i \leq r,\ 1 \leq j \leq l_i.$$

すると, M の固有多項式は $d_1(X)\cdots d_r(X)$, 最小多項式は $d_r(X)$, ジョルダン標準形は

$$\oplus_{i=1}^{r}(\oplus_{j=1}^{l_i} J(\alpha_{ij}, e_{ij}))$$

となる.

例 6.2.5 固有多項式が $(X-2)^3$ となる行列 M のジョルダン標準形の可能性を探ってみよう. $X \cdot I_3 - M$ は

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}, \quad d_1|d_2|d_3$$

に対等とする. このとき, $d_1d_2d_3 = (X-2)^3$ なので,

$$(d_1, d_2, d_3) = (1, 1, (X-2)^3),\ (1, X-2, (X-2)^2),\ (X-2, X-2, X-2)$$

と三通りの可能性がある. M のジョルダン標準形は, 順に,

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix},\quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix},\quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

となる.

例 6.2.6

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

に対し, 行列 $X \cdot I_3 - M$ は

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X+1)(X-2) \end{pmatrix}$$

に対等である. 従って M の固有多項式は $(X+1)(X-2)^2$ であり, 最小多項式は $(X+1)(X-2)$ に等しく, そのジョルダン標準形は

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

例 6.2.7

$$M = \begin{pmatrix} 4 & -4 & 4 \\ 1 & -1 & 4 \\ 0 & -1 & 4 \end{pmatrix}$$

に対し, 行列 $X \cdot I_3 - M$ は

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-3)(X-2)^2 \end{pmatrix}$$

に対等である. 従って M の固有多項式と最小多項式は共に, $(X-3)(X-2)^2$ に等しく, そのジョルダン行列は

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

第7章　多重線形射とテンソル積

7.1　多重線形射

7.1.1　定義と例

$V_1, \cdots, V_n, W$ を体 K 上の線形空間とし, それらの集合としての直積

$$V_1 \times \cdots\cdots V_n$$

を考える.

定義 7.1.1 写像

$$f : V_1 \times \cdots \times V_n \longrightarrow W; \quad (v_1, \cdots, v_n) \longmapsto f(v_1, \cdots, v_n)$$

は, 各 i $(1 \leq i \leq n)$ 番目の変数に関して, 線形射となるとき, 即ち, 次を満たすとき, **多重線形射** と呼ばれる：

$$f(v_1, \cdot, av_i + a'v_i', \cdots, v_n) = af(v_1, \cdot, v_i, \cdots, v_n) + a'f(v_1, \cdot, v_i', \cdots, v_n) \quad (\forall v_i \in V_i, \forall a, a' \in K).$$

特に, $W = K$ のとき, 多重線形射 f を **多重線形形式** という.
$n = 2$ のとき, **双線形射, 双線形形式** という. $n = 1$ のときは, 多重線形射は線形射に他ならないし, 多重線形形式は, 単に **線形形式** と呼ばれる.

例 7.1.1 n 縦数ベクトル空間 K^n の n 個の積からの写像

$$\det : K^n \times \cdots \times K^n \longrightarrow K \ (A_1, \cdots, A_n) \longmapsto \det(A_1, \cdots, A_n)$$

は, 多重線形形式である.

$V_1 \times \cdots \times V_n$ から W への多重線形形式全体の集合を

$$L := L(V_1, \cdots, V_n; W)$$

と表す. $f, g \in L, a, b \in L$ に対し,

$$(af + bg)(v_1, \cdots, v_n) = af(v_1, \cdots, v_n) + bg(v_1, \cdots, v_n) \quad (\forall (v_1, \cdots, v_n) \in V_1 \times \cdots \times V_n)$$

とすることにより, L は K 上の線形空間をなす.
$n = 1$ のときの $L(V; W)$ は, $\mathrm{Hom}_K(V, W)$ に他ならない.

問 7.1.2 $af + bg \in L(V_1, \cdots, V_n; W)$ を確かめよ.

7.1.2　双対空間と一次形式

V を K 上の線形空間とするとき, K 上の線形空間 $V^* := L(V;K) = \mathrm{Hom}_K(V,K)$ を, V の **双対空間** という. V^* の元を, V 上の **一次形式**, または, **線形汎関数** という.

$\mathcal{B} = (v_1, \cdots, v_n)$ を, V の基底とする. このとき, 補題　**??** により, 線形射 $v_i^* : V \longrightarrow K$ が存在し

$$v_i^*(v_j) = \delta_{ij} \quad (1 \leq i, j \leq n)$$

を満たす. このとき, $\mathcal{B}^* = (v_1^*, \cdots, v_n^*)$ は, V^* の基底をなし, $\mathcal{B}$ の **双対基底** と呼ばれる.

特に, $\dim(V) = \dim(V^*)$.

線形射 $f : V \longrightarrow W$ に対し, W 上の一次形式 l と f の合成写像 $l \circ f$ は, V 上の一次形式である.

$$f^* : W^* \longrightarrow V^*; \quad l \longmapsto l \circ f$$

は, 線形射である. f^* を f の **転置** という.

問 7.1.3 f^* が線形射であることを確かめよ.

$\mathcal{B} = (v_1, \cdots, v_n)$ を V の基底とし, $\mathcal{B}^* = (v_1^*, \cdots, v_n^*)$ をその双対基底とする. また, $\mathcal{C} = (w_1, \cdots, w_m)$ を W の基底とし, $\mathcal{C}^* = (w_1^*, \cdots, w_n^*)$ をその双対基底とする.

f の $\mathcal{B}$,$\mathcal{C}$ に関する表現行列を $A = (a_{ij}) \in \mathrm{M}_{m\times n}(K)$ とする: $f\mathcal{B} = \mathcal{C}A$.

このとき,

$$f^*(w_i^*)(v_j) = w_i^*(f(v_j) = w_i^*(\sum_{k=1}^{m} a_{kj} w_k) = a_{ij}$$

なので,

$$f^*(w_i^*) = \sum_{j=1}^{n} a_{ij} v_j^*.$$

従って,

$$f^*\mathcal{C}^* = \mathcal{B}^* {}^tA$$

を得る. 即ち, f^* の $\mathcal{C}^*, \mathcal{B}^*$ に関する表現行列は ${}^tA$ である.

例 7.1.2 単位行列の n 個列ベクトル $(e_1, \cdots, e_n)$ は, K^n の基底である.

$$e_i^* : K^n \longrightarrow K, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto x_i$$

とするとき, $(e_1^*, \cdots, e_n^*)$ が双対基底である.

問 7.1.4 V を線形空間とし, V^* をその双対とする. このとき,

$$\langle\ ,\ \rangle : V \times V^* \longrightarrow K; \quad (v, l) \longmapsto l(v)$$

は双線形形式であることを示せ.

補題 7.1.5 V を有限次元線形空間とする. $l(v) = 0$ $(\forall l \in V^*)$ ならば $v \in V$ は O である.

証明 $(v_1, \cdots, v_n)$ を V の基底とし, $(v_1^*, \cdots, v_n^*)$ をその双対基底とする. $v = \sum_i a_i v_i$ とすると, 仮定により, $v_j^*(v) = a_j = 0$ $(\forall j)$. 従って, $v = O$. □

V の任意の元 v に対し,

$$d(v) : V^* \longrightarrow K; \quad l \longmapsto l(v)$$

は, 線形射であり, V^* 上に一次形式である.

問 7.1.6 $d(v)$ が線形射であることを確かめよ.

定理 7.1.7 （有限次元線形空間の双対性）V を有限次元線形空間とするとき,

$$d : V \longrightarrow V^{**} = (V^*)^*; \quad v \longmapsto d(v)$$

は同型射である.

証明 $a, b \in K, u, v \in V$ に対し,

$$d(au + bv)(l) = l(au + bv) = al(u) + bl(v) = (ad(u) + bd(v))(l) \quad (\forall l \in V^*)$$

が成り立ち, $d(au + bv) = ad(u) + bd(v)$ を得る. 従って, d は線形射である.

$v \in \mathrm{Ker}(d)$ とすると, $d(v) = O$. 従って, 任意の $l \in V^*$ に対し, $d(v)(l) = l(v) = 0$. よって, 補題 7.1.5 より, $v = O$. 従って, $\mathrm{Ker}(d) = \{O\}$ となり, d は単射である. また, $\dim(V) = \dim(V^*) = \dim((V^*)^*)$ なので, 次元公式の系 **??** により, d は同型射である. □

7.2 テンソル積

この節では, 特に断らない限り, 体 K 上の有限次元線形空間を取り扱う.

7.2.1 テンソル積の定義

V, W を K 上の n, m 次元線形空間とし, $(v_1, \cdots, v_n), (w_1, \cdots, w_n)$ をそれぞれの基底とする. このとき, $\{v_i \otimes w_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ の一次結合

$$\sum_{i,j} a_{ij} v_i \otimes w_j \quad (a_{ij} \in K)$$

の全体 $V \otimes W$ を考える. 二つの一次結合

$$u = \sum_{i,j} a_{ij} v_i \otimes w_j, \quad u' = \sum_{i,j} a'_{ij} v_i \otimes w_j$$

が等しいとは, $a_{ij} = a'_{i,j}$ $(\forall i, j)$ のこととする. また, u, u' の和を

$$u + u' = \sum_{i,j} (a_{ij} + a'_{ij}) v_i \otimes w_j$$

と定め, スカラー倍を

$$c \cdot u = \sum_{ij} ca_{ij} v_i \otimes w_j$$

と定めると, $(V \otimes W; +, \cdot)$ は, K 上, $(v_i \otimes w_j)$ を基底とする mn 次元の線形空間をなす. これを, $V \otimes W$ と表し, V と W の K 上の **テンソル積** という.

$v = \sum_i a_i v_i \in V, \sum_j b_j w_j \in W$ に対し,

$$v \otimes v = \sum_{ij} a_i b_j v_i \otimes w_j \in V \otimes W$$

を, v と w の **テンソル積** という.

例 7.2.1 線形空間 V と 1 次元線形空間 K に対し,

$$V \longrightarrow V \otimes K \quad v \longmapsto v \otimes 1$$

は同型射である. この同型射により, V と $V \otimes K$ を同一視する.

補題 7.2.1 写像

$$\otimes = \otimes_{V,W} : V \times W \longrightarrow V \otimes W; \quad (v, w) \longmapsto v \otimes w$$

は双線形射である. 特に, $a(v \otimes w) = (av) \otimes w = v \otimes aw$ が成り立つ.

証明 $v' = \sum_i a'_i v_i \in V$ とし, $c, c' \in K$ とするとき,

$$\begin{aligned}
(cv + cv') \otimes w &= (\sum_i (ca_i + ca'_i) v_i) \otimes (\sum_j b_j w_j \\
&= \sum_{i,j} (ca_i + ca'_i) b_j (v_i \otimes w_j) \\
&= c(\sum_{i,j} a_i b_j v_i \otimes w_j) + c \sum_{i,j} a'_i b_j v_i \otimes w_j) \\
&= cv \otimes w + c'v' \otimes w.
\end{aligned}$$

同様にして, $v \otimes (cw + c'w') = c\, v \otimes w + c'v \otimes w'$ を得る. □

次は, やや冗長のきらいはあるが, 後に一般の場合のテンソル積の理解に資する為である.

線形空間 U と双一次形式 $\Phi : V \times W \longrightarrow U$ の組 (U, Φ) が, 次の性質を持つとき, 双線形射 $V \times W \longrightarrow T'$ に関する ddot 普遍性 ddot を持つという：

$f : V \times W \longrightarrow T'$ を任意の双線形射とするとき, 次の図を可換にする線形射 $\tilde{f} : U \longrightarrow T'$ が唯一つ存在する：

$$\begin{array}{ccc}
 & otimes & \\
V \times W & \longrightarrow & U \\
f \searrow & & \swarrow \tilde{f} \\
 & T'. &
\end{array}$$

定理 7.2.2 $(V \otimes W, \otimes)$ は普遍性を持つ. (U, Φ) も普遍性を持てば, $\phi \circ \otimes = \Phi$ を満たす同型射 $\phi : V \otimes V \longrightarrow U$ が一意的に存在する.

証明 $f : V \times W \longrightarrow T'$ を任意の双線形射とするとき, $\tilde{f}(v_i \otimes w_j) = f(v_i, w_j)$ と定めれば, 補題 **??** により, 線形射 $\tilde{f} : V \otimes W \longrightarrow T'$ を得て, $\tilde{f} \circ \otimes = f$ を満たす. 線形射 $g : V \otimes W \longrightarrow T'$ も $g \circ \otimes f$ を満たすとすると, $f(v_i, w_j) = g(v_i \otimes w_j)$ が成り立つので, $\tilde{f} = g$ を得る. よって, $(V \otimes W, \otimes)$ は普遍性を満たす.

$(V \otimes W, \otimes)$ の普遍性より, $\tilde{\Phi} \circ \otimes = \Phi$ を満たす線形射 $\tilde{\Phi} : V \otimes W \longrightarrow U$ が唯一つ存在する. また, (U, Φ) の普遍性より, $\tilde{\otimes} \circ \Phi = \otimes$ を満たす線形射 $\tilde{\otimes} : U \longrightarrow V \otimes W$ が唯一つ存在する. このとき, 普遍性より, $\tilde{\phi} \circ \tilde{\otimes} = I_U, \tilde{\otimes} \circ \tilde{\phi} = I_{V \otimes W}$ を得る. よって, $\tilde{\Phi}, \tilde{\otimes}$ は同型射であり互いに他の逆写像である. □

命題 7.2.3

$$V \otimes W \longrightarrow W \otimes V; \quad v \otimes w \longmapsto w \otimes v$$

は同型射である.

証明 写像

$$\Phi : V \times W \longrightarrow W \otimes V; \quad (v, w) \longmapsto w \otimes v$$

は双線形射である. このとき, $(W \otimes V, \Phi)$ は普遍性を持つ. 実際, $f : V \times W \longrightarrow T'$ を任意の双線形射とするとき, $\tilde{f}(w_j \otimes v_i) = f(v_i, w_j)$ と定めれば, 線形射 $\tilde{f} : W \otimes V \longrightarrow T'$ を得て, $\tilde{f} \circ \Phi = f$ を満たす. $\tilde{f}$ の一意性も, 定理の証明と同様である.

従って, 定理より, 同型射 $\phi : V \otimes W \longrightarrow W \otimes V$ が存在し, $\phi \circ \otimes = \Phi$ を満たす. よって,

$$\phi(v \otimes w) = \Phi(v, w) = w \otimes v$$

を得て, 命題が示された. □

命題 7.2.4 U, V, W を線形空間とするとき,

$$\psi : U \otimes (V \otimes W) \simeq (U \otimes V) \otimes W; \quad u \otimes (v \otimes w) \longmapsto (u \otimes v) \otimes w$$

は同型射である.

問 7.2.5 命題を証明せよ.

次の定理も, 以前と同様にして, 容易に得られる.

定理 7.2.6 $V_1, \cdots, V_k$ を線形空間とするとき, $V_1 \otimes \cdots V_k$ と多重線形射

$$\otimes : V_1, \cdots, V_k \longrightarrow V_1 \otimes \cdots V_k; \quad (v_1, \cdots, v_k) \longmapsto v_1 \otimes \cdots \otimes v_k$$

の組 $(V_1 \otimes \cdots V_k, \otimes)$ は普遍性を持つ. 即ち, 任意の多重線形射 $\Phi : V_1 \times \cdots \times V_k \longrightarrow T'$ に関して, $\tilde{\Phi} \circ \otimes = \Phi$ を満たす線形射 $\phi : V_1 \otimes \cdots V_k \longrightarrow T'$ が一意的に存在する.

定理-定義 7.2.7 $f : V \longrightarrow V', g : W \longrightarrow W'$ を線形射とすると,

$$(f \otimes g)(v \otimes w) = f(v) \otimes g(w) \quad (\forall (v, w) \in V \times W)$$

を満たす線形射

$$f \otimes g : V \otimes W \longrightarrow V' \otimes W'$$

が一意的に存在する.

$f \otimes g$ を f と g の **テンソル積** という.

証明　写像

$$\Phi : V \times W \longrightarrow V' \otimes W' \quad (v, w) \longmapsto f(v) \otimes g(w)$$

は双線形射である. 従って, テンソル積の普遍性（定理 **??**）により, $\tilde{\Phi} \circ \otimes_{V,W} = \Phi$ を満たす線形射 $\tilde{\Phi} : V \otimes W \longrightarrow V' \otimes W'$ が一意的に存在する. $\tilde{\Phi} = f \otimes g$ とすれば良い. このとき, $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ を満たす. □

$\mathcal{B} = (v_1, \cdots, v_n), \mathcal{B}' = (v'_1, \cdots, v'_{n'})$ を, V, V' の基底とし, $\mathcal{C} = (w_1, \cdots, w_m), \mathcal{C}' = (w'_1, \cdots, w'_{m'})$ を, W, W' の基底とする. 線形射 $f : V \longrightarrow V', g : W \longrightarrow W'$ の, これらの基底に関する表現行列を A, B とする：

$$f\mathcal{B} = \mathcal{B}'A, \quad g\mathcal{B} = \mathcal{B}'B \quad (A = (a_{ij}) \in \mathrm{M}_{n \times n'}(K), B = (b_{kl}) \in \mathrm{M}_{n \times n'}(K).$$

このとき,

$$\mathcal{D} = (v_i \otimes w_j), \mathcal{D}' = (v'_i \otimes w'_j)$$

は, $V \otimes W, V' \otimes W'$ の基底である.

$$\begin{aligned} (f \otimes g)(v_i \otimes v_j) &= (\sum_k a_{ki} v'_k) \otimes (\sum_l b_{lj} w'_l) \\ &= \sum_{k'l'} a_{k'i} b_{l'j} (v'_k \otimes w'_l) \end{aligned}$$

なので, これらの基底に関する $f \otimes g$ の表現行列は $A \otimes B$ である. 但し, $A \otimes B$ の (k', l') 行 (i, j) 列成分は

$$a_{k'i} b_{l'j}$$

である $n'm' \times nm$ 行列である. 基底 $\mathcal{D}, \mathcal{D}'$ の順序を

$$(1,1), \cdots, (n,1), (1,2), \cdots, (n,2), \cdots, (n-1,m), (n,m),$$

$$(1,1), \cdots, (n',1), (1,2), \cdots, (n',2), \cdots, (n'-1,m'), (n',m')$$

とすれば,

$$A \otimes B = \begin{pmatrix} Ab_{11} & Ab_{12} & \cdots & Ab_{1m} \\ Ab_{21} & Ab_{22} & \cdots & Ab_{2m} \\ \vdots & \vdots & & \vdots \\ Ab_{m'1} & Ab_{m'2} & \cdots & Ab_{m'm} \end{pmatrix} \in \mathrm{M}_{n'm' \times nm}(K)$$

となる. $A \otimes B$ を行列 A と B の **Kronecker 積** という.

7.2.2 テンソル積と多重線形射

テンソル積と双対空間の関係から始めよう.

定理 7.2.8 V, W を線形空間とするとき,

$$V^* \otimes W^* \longrightarrow (V \otimes W)^* \quad \phi \otimes \psi \longmapsto \phi\psi$$

は同型射である. 但し, $\phi\psi(v \otimes w) = \phi(v)\psi(w)$ $(\forall v \otimes w)$.

証明 $(\phi, \psi) \in V^* \times W^*$ に対し,

$$V \times W \longrightarrow K \quad (v, w) \longmapsto \phi(v)\psi(w)$$

は双線形形式なので, テンソル積の普遍性により, 線形射 $\Phi(\phi, \psi) : V \otimes W \longrightarrow K$ が存在し, $\Phi(\phi, \psi)(v \otimes w) = \phi(v)\psi(w)$ を満たす. すると,

$$\Phi : V^* \times W^* \longrightarrow (V \otimes W)^*$$

は双線形射である. 再び, テンソル積の普遍性により, $f \circ \otimes f = \Phi$ を満たす線形射 $f : V^* \otimes W^* \longrightarrow (V \otimes W)^*$ が一意的に存在する.

$(v_i), (w_j)$ を V, W の基底とし, $(v_i^*), (w_j^*)$ をそれらの双対基底とする. さて, $l := \sum_{ij} a_{ij} v_i^* \otimes w_j^* \in \mathrm{Ker}(f)$ とすると, $l(v_i \otimes w_j) = a_{ij} = 0$ $(\forall (i, j))$ なので, $l = 0$. 従って, f は単射であり, 次元を比べて, 同型射であることが判る. □

写像

$$V^* \times W \longrightarrow \mathrm{Hom}(V, W) \quad l \otimes w \longmapsto (v \mapsto l(v)w)$$

は双線形射である. 従って, テンソル積の普遍性により,

$$f(l \otimes w) = (v \mapsto l(v)w)$$

を満たす線形射 $f : V^* \times W \longrightarrow \mathrm{Hom}(V, W)$ が一意的に存在する. このとき, f は単射であり, $\dim(\mathrm{Hom}(V, W)) = \dim(V)\dim(W)$ なので, f は同型射となる. よって, 次の定理を得る：

定理 7.2.9

$$V^* \times W \longrightarrow \mathrm{Hom}(V, W) \quad l \otimes w \longmapsto (v \mapsto l(v)w)$$

は同型射である.

定理 7.2.10

$$L(V_1 \times \cdots \times V_k; W) \simeq \mathrm{Hom}(V_1 \otimes \cdots \otimes V_k, W) \simeq V_1^* \otimes \cdots \otimes V_k^* \otimes W.$$

問 7.2.11 定理において, $l_1 \otimes \cdots \otimes l_k \otimes w$ と多重線形射 $F : (v_1, \cdots, v_k) \longmapsto l_1(v_1) \cdots l_k(v_k)w$ が対応することを確かめよ.

定義 7.2.12 V を n 次元線形空間とする.

$$\begin{aligned} T^{p,q} &= \overbrace{V^* \otimes \cdots \otimes V^*}^{p} \otimes \overbrace{V \otimes \cdots \otimes V}^{q} \\ &= \left(\overbrace{V \otimes \cdots \otimes V}^{p} \otimes \overbrace{V^* \otimes \cdots \otimes V^*}^{q} \right)^* \end{aligned}$$

を p-階 **共変**, q-階 **反変** である $p+q$**-階テンソル空間** という. $p > 0$ かつ $q > 0$ を満たすテンソルを **混合テンソル** という.

例 7.2.2 2 階の混合テンソル空間は,

$$\mathrm{Hom}_K(V,V) = \mathrm{End}_K(V) = V^* \otimes V.$$

2 階の共変テンソル空間は, V 上の双一次形式のなす空間である：

$$L(V \times V, K) = \mathrm{Hom}_K(V \otimes V, K) = V^* \otimes V^*.$$

共変, 反変の意味については, 後小節を参照のこと.

7.2.3　テンソル代数

V を体 K 上の n 次元線形空間とする. V の r 個のテンソル積 $T^r(V)$ の無限個の直和を

$$\mathbb{T}(V) = \oplus_{r=0}^{\infty} T^r(V) \quad (T^0(V) = K, T^1(V) = V)$$

と表す. 即ち, 有限個のテンソルの K 上の一次結合

$$\sum a_r \tau_r \quad (\tau_r \in T^r(V))$$

全体のなす（無限次元）線形空間を $T(V)$ と表す.

二つのテンソル

$$t_r = x_1 \otimes \cdots \otimes x_r \in T^r(V), \quad t_s = y_1 \otimes \cdots \otimes y_s \in T^s(V)$$

に対し, その積を

$$t_r \cdot t_s = x_1 \otimes \cdots \otimes x_r \otimes y_1 \otimes \cdots \otimes y_s \in T^{r+s}(V)$$

と定めることにより, $(T(V); +, \cdot)$ は環をなす. 更に, 環単射

$$\iota : K \longrightarrow T(V); \quad c \longmapsto c \in K = T^0 \subset T(V)$$

により, $T(V)$ は, K 上の線形空間をなしている：即ち, $t \in T(V)$ の $c \in K$ 倍が, $c \cdot t = \iota(c)t$ で定められている. 環 $T(V)$ と環単射 ι の組 $(T(V), \iota)$ は, K 上の代数である.

線形射 $\tau : V \longrightarrow T(V)$ を, $\tau(v) = v$ により定め, 組 $(T(V), \tau)$ を, V の **テンソル代数** という.

を V の **テンソル代数** という.

定理 7.2.13 （テンソル代数の普遍性）K 上の代数 $A=(A,\iota_A)$ と線形射 $\alpha : V \longrightarrow A$ の組 (A,α) に対し, $\alpha_* \circ \tau = \alpha$ を満たす代数射 $\alpha_* : T(V) \longrightarrow A$ が唯一つ存在する.

$(T(V),\tau)$ は, 同型を除いて, この性質を持つ唯一の組である.

証明 $(x_1,\cdots,x_r)$ に対し, $\alpha(x_1)\cdots\alpha(x_r)$ を対応させる写像は, α が線形射であり, A が代数なので, 多重線形射 $V^r = V\times\cdots\times V \longrightarrow A$ である. 従って, テンソルの普遍性により,

$$\alpha_*(x_1\otimes\cdots\otimes x_r)=\alpha(x_1)\cdots\alpha(x_r)$$

を満たす線形射 $\alpha_* : T^r(V) \longrightarrow A$ が一意的に存在する. よって, $\alpha_*(c)=\iota_A(c)$ $(c\in K)$ とすることにより, 線形射 $\alpha_* : T(V) \longrightarrow A$ を得る.

$$\alpha_*\left((x_1\otimes\cdots\otimes x_r)(y_1\otimes\cdots\otimes y_s)\right) \\ = \alpha(x_1)\otimes\cdots\otimes\alpha(x_r)\alpha(y_1)\otimes\cdots\otimes\alpha(y_s)$$

なので, α_* は代数射である. 一意性は明らかである.

普遍性より, 定理 **??** と同様にして, 後半が示される. □

r 次対称群 S_r は, 次のようにして, テンソル空間 $T^r(V)$ に作用する：

$\sigma\in S_n$ とする. このとき,

$$V^r \longrightarrow T^r(V) \quad (x_1,\cdots x_r)\longmapsto x_{\sigma(1)}\otimes\cdots\otimes x_{\sigma(r)}$$

は多重線形射である. 従って, テンソル積の普遍性により, 線形射

$$P_\sigma : T^r(V)\longrightarrow T^r(V) \quad (x_1\otimes\cdots\otimes x_r)=x_{\sigma(1)}\otimes\cdots\otimes x_{\sigma(r)}$$

が存在する. このとき,

$$\begin{aligned} P_\sigma P_\tau(x_1\otimes\cdots\otimes x_r) &= P_\sigma(x_{\tau(1)}\otimes\cdots\otimes x_{\tau(r)} \\ &= x_{\sigma(\tau(1))}\otimes\cdots\otimes x_{\sigma(\tau(r))} \\ &= P_{\sigma\tau}(x_1\otimes\cdots\otimes x_r) \end{aligned}$$

が成り立ち,

$$P_{\sigma\tau}=P_\sigma P_\tau$$

を得る.

定義 7.2.14 $t_r\in T^r(V)$ が

$$P_\sigma(t_r)=\begin{cases} t_r & \\ \mathrm{sign}(\sigma)t_r & (\forall\sigma\in S_r)\end{cases}$$

を満たすとき, t_r を, それぞれ, **対称テンソル**, **歪対称テンソル** という.

また, 任意の互換 τ に対し,

$$P_\tau(t_r)=0$$

を満たす t_r を **交代テンソル** という.

問 7.2.15 交代テンソルは, 歪対称テンソルであることを示せ. また, K の標数が 2 でない, 即ち, $1+1\neq 0$ ならば, 歪対称テンソルは交代テンソルであることを示せ.

7.3　外積代数

V を体 K 上の n 次元線形空間とするとき, V の双対空間 V^* の p 個のテンソル積空間 $T^p(V^*)$ を p-階共変テンソル空間といった.

7.3.1　外積代数の定義

W を体 K 上の n 次元空間とし, $(f^1, \cdots, f^n)$ を基底とする. $I = \{1, \cdots, n\}$ とし, I の部分集合 S に対し, 記号 f^S を定める. 但し, $f^\emptyset = 1$ と表す. $\{f^S \mid S \subset I\}$ を基底とする 2^n 次元線形空間を $\Lambda.W$ と表す. すると, $\Lambda.W$ は, 部分空間

$$\Lambda_r(W) = \langle f^S \mid |S| = r \rangle$$

の直和と表される：

$$\Lambda.W = \Lambda_0(W) \oplus \Lambda_1 W \oplus \Lambda_2(W) \oplus \cdots \oplus \Lambda_n W.$$

例 7.3.1 $1 = f^\emptyset$ と体 K の単位元 1, $f^{\{i\}}$ と f^i を同一視して,

$$\Lambda_0 W = K, \quad \Lambda_1 W = W.$$

$S, T \subset I$ に対し,

$$k(S,T) = \{(i,j) \mid i \in S, j \in T, i > j\}$$

と定め,

$$\epsilon(S,T) = \begin{cases} (-1)^{|k(S,T)|} & S \cap T = \emptyset \\ 0 & S \cap T \neq \emptyset \end{cases}$$

と定める. そこで,

$$f^S \wedge f^T = \epsilon(S,T) f^{S \cup T}$$

と定義すると, 線形性により, $\Lambda.W$ の二項演算 $\wedge$ が定まり, $(\Lambda.W; +, \wedge)$ は環をなす. $\Lambda.W$ と環単射 $\iota : K \longrightarrow \Lambda.W$ の組 $(\Lambda.W, \iota)$ は K 上の代数である.

例 7.3.2

$$1 \wedge e^S = e^S \quad (\forall S \subset I),$$

$$f^i \wedge f^i = 0, \quad f^j \wedge f^i = -f^i \wedge f^j \ (i \neq j).$$

例題 7.3.1 $R, S, T \subset I$ に対し,

$$(f^R \wedge f^S) \wedge f^T = f^R \wedge (f^S \wedge f^T)$$

を確かめよ.

（解） R, S, T のいずれか二つが, 交われば, 両辺が 0 となり等しい. そこで, これらは互いに交わらないとする. このとき,

$$k(R \cup S, T) = k(R, T) + k(S, T), \quad k(R, S \cup T) = k(R, S) + k(R, T)$$

と直和になることに注意する. すると,

$$\begin{aligned}(f^R \wedge f^S) \wedge f^T &= \epsilon(R, S) f^{R \cup S} f^T \\ &= \epsilon(R, S)\epsilon(R \cup S, T) f^{R \cup S \cup T} \\ &= (-1)^{|k(R,S|+|k(R,T)|+|k(S,T)|} f^{R \cup S \cup T} \\ &= f^R \wedge (f^S \wedge f^T)\end{aligned}$$

を得る. □

例 7.3.3 $i_1 < \cdots < i_r$ のとき, $S = \{i_1, \cdots, i_r\}$ とすれば

$$f^{i_1} \wedge \cdots \wedge f^{i_r} = f^S.$$

f^i に $f^{\{i\}} (= f^i)$ を対応させることにより, 線形射

$$\lambda : W \longrightarrow \Lambda.W$$

を得る. λ は,

$$\lambda(w) \wedge \lambda(w) = 0 \quad (\forall w \in W)$$

を満たす. 代数 $\Lambda.W$ と λ の組 $(\Lambda.W, \lambda)$ を, W の **外積代数** という.

次の普遍性は, 定理 6.1.4 と同様にして示される.

定理 7.3.2 （外積代数の普遍性）K 上の代数 A と, $\alpha(w)^2 = 0$ $(\forall w \in W)$ を満たす線形射 $\alpha : W \longrightarrow A$ の組 (A, α) に対し, $\alpha_* \circ \lambda = \alpha$ を満たす代数射 $\alpha_* : \Lambda.(W) \longrightarrow A$ が唯一つ存在する.

$(\Lambda.W, \lambda)$ は, 同型を除いて, この性質を持つ唯一の組である.

問 7.3.3 定理を証明せよ.

問 7.3.4 $\xi \in \Lambda_k W, \eta \in \Lambda_l W$ に対し,

$$\xi \wedge \eta = (-1)^{kl} \eta \wedge \xi$$

が成り立つことを示せ.

p-ベクトルのなす部分空間 $\Lambda_p W$ の普遍性を考察する.

$$\wedge_p : W^p \longrightarrow \Lambda_p W; \quad (\xi^1, \cdots, \xi^p) \longmapsto \xi^1 \wedge \cdots \wedge \xi^p$$

は交代多重線形射である. 即ち, 多重線形射であり,

$$\xi^1 \wedge \cdots \wedge \xi^p = 0 \quad (\xi^i = \xi^j \ (i \neq j)$$

を満たす. このとき, 組 $(\Lambda_p W, \wedge_p)$ は, 次の普遍性を持つ. その証明は, 行列式の特徴付けの証明の類似である：

定理 7.3.5（p-ベクトル空間の普遍性）$D : W^r \longrightarrow U$ を交代多重線形射とするとき, $D_* \circ \wedge_p = D$ を満たす線形射 $D_* : \Lambda_p W \longrightarrow U$ が一意的に存在する.

$(\Lambda_p W, \wedge_p)$ は, 同型を除いて, この性質を持つ唯一の組である.

証明　$D_*(f^S) = D(f^{i_1}, \cdots, f^{i_p})$ により, 線形射 $D_* : \Lambda_p W \longrightarrow U$ を定める. すると,

$$\xi^i = \sum_{j=1}^{n} a^i_j f^j \quad (1 \leq i \leq p)$$

に対し,

$$\begin{aligned} D_*(\xi^1 \wedge \cdots, \wedge \xi^p) &= (\sum_j a^j_1 f^j) \wedge \cdots (\sum_j a^j_p f^j) \\ &= \sum_{j_1, \cdots, j_p} a_{1j_1} \cdots a_{pj_p} f^{j_1} \wedge \cdots f^{j_n} \\ &= \sum_{j_1, \cdots, j_p, \neq} a_{1j_1} \cdots a_{pj_p} f^{j_1} \wedge \cdots f^{j_p} \end{aligned}$$

を得る. ここで, $S = \{j_1, \cdots, j_p\} = \{i_1 < \cdots < i_p\}$ とすれば,

$$\begin{aligned} D_S &:= \det \begin{pmatrix} a^1_{i_1} & \cdots & a^1_{i_p} \\ \vdots & & \vdots \\ a^p_{i_1} & \cdots & a^p_{i_p} \end{pmatrix} \\ &= \sum_{S=\{j_1, \cdots, j_p\}} \operatorname{sign} \begin{pmatrix} i_1 & \cdots & i_p \\ j_1 & \cdots & j_p \end{pmatrix} a_{1j_1} \cdots a_{pj_p} \end{aligned}$$

を得る. 従って,

$$D_*(\xi^1 \wedge \cdots, \wedge \xi^p) = \sum_S D_S f_S.$$

同様にして,

$$D(\xi^1, \cdots, \xi^p) = \sum_S D_S D(f^{i_1}, \cdots, f^{i_p})$$

を得る. よって, $D_* : \Lambda_p W \longrightarrow U$ が成り立つ.

一意性は明らかであり, 後半の証明は, いつもの通り. □

線形射 $\phi : W \longrightarrow W'$ に対し, $\Lambda.W'$ において, $\phi(w) \wedge \phi(w) = 0$ $(\forall w \in W)$ が成り立つ. 従って, 外積代数 $\Lambda.W$ の普遍性により, 代数射

$$\Lambda.\phi : \Lambda.W \longrightarrow \Lambda.W'; \quad w_1 \wedge \cdots \wedge w_k \longmapsto \phi(w_1) \wedge \cdots \wedge \phi(w_k)$$

を得る. $\Lambda.\phi$ の $\Lambda_k W$ への制限は, 線形射

$$\Lambda_k \phi : \Lambda_k W \longrightarrow \Lambda_k W'$$

を得る.

例題 7.3.6 $\phi : W \longrightarrow W$ を線形射とする. このとき,

$$(\Lambda_n \phi) f^I = \det(\phi) f^I$$

が成り立つことを示せ.

（解） 線形射 ϕ の基底 (f^i) に関する表現行列を $A = (a_i^j)$ とする：$\phi(f^i) = A(f^i)$. このとき,

$$\begin{aligned}(\Lambda.\phi)(f^I) &= \phi(f^1) \wedge \cdots \wedge \phi(f^n) \\ &= (\sum_j a_1^j f^j) \wedge \cdots (\sum_j a_n^j f^j) \\ &= \sum_{j_1,\cdots,j_n} a_{1j_1} \cdots a_{nj_n} f^{j_1} \wedge \cdots f^{j_n} \\ &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdots a_{n\sigma(n)} f^{\sigma(1)} \wedge \cdots f^{\sigma(n)}\end{aligned}$$

を得る. 補題 **??** より, 置換の符号と互換の関係を考慮して,

$$f^{\sigma(1)} \wedge \cdots f^{\sigma(n)} = \mathrm{sign}(\sigma) f^1 \wedge \cdots f^n.$$

従って, 行列式の完全展開（定理 **??**）より, 結論を得る. □

7.3.2 双対と共役ベクトル

W^* を W の双対空間とする.

補題 7.3.7

$$v = v_1 \wedge \cdots \wedge v_p \in \Lambda_p W^*, \quad \xi = \xi^1 \wedge \cdots \wedge \xi^p \in \Lambda_p W$$

に対し,

$$\langle \xi, v \rangle = \det(v_i(\xi^j))$$

を満たす双線形形式

$$\langle\ ,\ \rangle : \Lambda_p W \times \Lambda_p W^* \longrightarrow K$$

が存在する.

証明 $(v_1, \cdots, v_p) \in \Lambda_p(W^*)$ を固定すると,

$$W^p \longrightarrow K; \quad (\xi^1, \cdots, \xi^p) \longmapsto \det(v_i(\xi^j))$$

は交代多重線形形式である. 従って, $\Lambda_p W$ の普遍性により, 線形形式

$$\Lambda_p W \longrightarrow K; \quad \xi^1 \wedge \cdots \wedge \xi^p \longmapsto \det(v_i(\xi^j))$$

が一意的に定まる. 次に, $\xi = \xi^1 \wedge \cdots \wedge \xi^p \in \Lambda_p W$ を固定すると,

$$(W^*)^p \longrightarrow K; \quad (v_1, \cdots, v_p) \longmapsto \det(v_i(f^j))$$

も交代多重線形形式なので, $\Lambda_p(W^*)$ の普遍性により, 線形形式

$$\Lambda_p(W^*) \longrightarrow K \quad v_1 \wedge \cdots \wedge v_p \longmapsto \det(v_i(f^j))$$

を得る. これらを組み合わせて, 補題の結論を得る. □

$(e_1, \cdots, e_n)$ を W の基底 (f^i) の双対基底とし, $S = \{i_1 < \cdots < i_p\} \subset I$ に対し,

$$e_S = e_{i_1} \wedge \cdots \wedge e_{i_p}$$

と定める.

$|S| = |T| = p$ を満たす I の部分集合 S, T に対し,

$$\langle f^S, e_T \rangle = \det(e_{i_k}(f^{j_l})) = \delta_{S,T}$$

が成り立ち, $\langle\ ,\ \rangle$ は非退化である. 従って,

$$\Lambda_p(W^*) \longrightarrow (\Lambda_p W)^*; \quad e_S \longmapsto (f^T \mapsto \langle e_S, f^T \rangle)$$

は同型射である. この同型射により, $\Lambda_p(W^*)$ と $(\Lambda_p W)^*$ を同一視すれば, $(\cdots, e_S, \cdots)$ が $\Lambda_p W$ の基底 (f^S) の双対基底である.

$\Lambda_n W$ の基底 f^I を固定する. $\alpha \in \Lambda_p W, \xi \in \Lambda_{n-p} W$ に対し,

$$\alpha \wedge \xi = (\alpha, \xi) f^I \quad (\alpha, \xi) \in K$$

と表される. このとき,

$$\Lambda_p W \times \Lambda_{n-p} W \longrightarrow K \longrightarrow (\alpha, \xi)$$

は双線形形式である. $S \subset I$ $(|S| = p)$ に対し, $T = I - S$ とすれば, $(f^S, f^T) f^I = f^S \wedge f^T = \epsilon(S, T) f^I$ なので, $(f^S, f^T) = \epsilon(S, T) \neq 0$ なので, $(\ ,\ )$ は非退化である. 従って,

$$\Lambda_p W \longrightarrow (\Lambda_{n-p} W)^*; \alpha \longmapsto (\xi \mapsto (\alpha, \xi)$$

は同型射である.

さて, $e_T \longmapsto f^T$ により, $\Lambda_{n-p}(W^*)$ と $\Lambda_{n-p}(W)$ を同一視する. このとき, 二つの同型射の合成写像を

$$* : \Lambda_p W \longrightarrow (\Lambda_{n-p} W)^* \longrightarrow \Lambda_{n-p}(W^*) = \Lambda_{n-p} W$$

と表すと

$$\langle \xi, * \alpha \rangle = (\alpha, \xi) \quad (\forall \xi \in \Lambda_{n-p} W),$$

即ち,

$$* \alpha \wedge \xi = \langle \xi, * \alpha \rangle f^I$$

が成り立つ. $* \alpha \in \Lambda_{n-p}(W^*)$ を $\alpha \in \Lambda_p W$ の **共役ベクトル** という.

例題 7.3.8 $S \subset I$ $(|S| = p)$ のとき, $* f^S = \epsilon(S, I - S) f^{I-S}$ であることを示せ.

（解） $*f^S = \sum_{T\subset I,|T|=n-p} a_T f^T$ とする. このとき, 任意の f^R $(|R| = n-p)$ に対し,

$$\begin{aligned}\epsilon(S,R)f^{S\cup R} &= f^S \wedge f^R = (f^S, f^R)f^I \\ &= \langle f^R, *f^S\rangle f^I = a_R f^I.\end{aligned}$$

従って, $R = I - S$ のとき, $a_{I-S} = \epsilon(S, I-S)$ であり, $R \neq I-S$ のとき, $a_R = 0$. よって, $*f^S = \epsilon(S, I-S)f^{I-S}$ を得る. □

例 7.3.4 $n = 3, p = 2$ のとき,

$$*f^{\{1,2\}} = f^3,\ *f^{\{1,3\}} = -f^2,\ *f^{\{2,3\}} = f^1.$$

7.3.3 三次元 Euclid 線形空間の内積と外積

この小節は, 物理学に於けるベクトル解析の基本事項の解説を意図するので, 表記法もそれに倣うことにする. 三次元ユークリッド線形空間の基底を $\mathbf{i}, \mathbf{j}, \mathbf{k}$ と表すことが多いが, その由来を解説する

実数と虚数単位 i を用いて複素数を構成したことを拡張することから始めよう. 今度は虚数単位を三個用意し, それを $\mathbf{i}, \mathbf{j}, \mathbf{k}$ とし,

$$\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \quad (a, b, c, d \in \mathbb{R})$$

を **四元数** という. 勿論, 二つの四元数が等しいとは, 各係数が等しいこととする：

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k} \qquad \Longleftrightarrow \quad a = a', b = b', c = c', d = d'.$$

四元数の全体を $\mathbb{H}$ と表す. 二つの四元数の和を

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k} = (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$$

と定める. 積については, まず, 実数 e と四元数の積を

$$e \cdot (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})e = ea + eb\mathbf{i} + ec\mathbf{j} + ed\mathbf{k}$$

と定める. すると, $(\mathbb{H}; +, \cdot)$ は, $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ を基底とする四次元実線形空間をなす.

問 7.3.9 これを確かめよ.

次に, 虚数単位同士の積を

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}$$

と定める. 積に関して結合法則が成り立つとすると, 虚数単位同士の積は全て定まる. 例えば,

$$(-1)\mathbf{ji} = \mathbf{i}^2\mathbf{ji} = \mathbf{iki} = \mathbf{ij} = \mathbf{k}$$

となり, $\mathbf{ji} = -\mathbf{k}$ を得る. 従って, 積に関して可換ではない.

問 7.3.10

$$\mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}$$

を示せ.

二つの四元数の積は, 結局,

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = A + Bi + Cj + Dk,$$

$$A = aa' - bb' - cc' - dd', \quad B = ab' + ba' + cd' - dc',$$
$$C = ac' + ca' + db' - bd', \quad D = ad' + da' + bc' - cb'$$

となる. すると, $(\mathbf{H}; +, \cdot)$ は $\mathbb{R}$-代数をなし, **Hamilton の四元数環** と呼ばれる.

四元数 $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ に対し,

$$\bar{q} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

を, q の共役といい,

$$N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2, \quad T(q) = q + \bar{q} = 2a$$

を q の **ノルム**, **トレース** という. 更に,

$$\mathrm{Re}(q) = \frac{1}{2}(q + \bar{q}) = a, \quad \mathrm{Im}(q) = \frac{1}{2}(q - \bar{q}) = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

を q の **実部**, **虚部**という.

共役に関して,

$$\overline{q\bar{q}'} = \bar{q}'\bar{q}$$

に注意する. また, $q \neq 0$ ならば, $q^{-1} = N(q)^{-1}\bar{q}$ であり, $\mathbb{H}$ は斜体, 即ち, 非可換な体である.

Hamilton の四元数環の虚部

$$V = \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k}$$

を, 三次元実線形空間 $\mathbb{R}^3$ と同一視する：

$$x\mathbf{i} + y\mathbf{j} + z\mathbf{k} \longleftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

純虚ベクトルに対し,

$$\bar{\mathbf{a}} = -\mathbf{a}, \quad \overline{\mathbf{ab}} = \mathbf{ba} \tag{7.1}$$

が成り立つことに注意する.

二つのベクトル $\mathbf{a} = a_x\mathbf{i} + a_y\mathbf{j} + a_z\mathbf{k}, \mathbf{b} = b_x\mathbf{i} + b_y\mathbf{j} + b_z\mathbf{k}$ を四元数の虚部と見なして積を取ると

$$\mathbf{ab} = -(a_xb_x + a_yb_y + a_zb_z) + (a_yb_z - a_zb_y)\mathbf{i} + (a_zb_x - a_xb_z)\mathbf{j} + (a_xb_y - a_yb_x)\mathbf{k}.$$

そこで, $\mathbf{a}$ と $\mathbf{b}$ との **内積**, **外積** を

$$\mathbf{a}\cdot\mathbf{b} = a_xb_x + a_yb_y + a_zb_z,$$

$$\mathbf{a}\times\mathbf{b} = (a_yb_z - a_zb_y)\mathbf{i} + (a_zb_x - a_xb_z)\mathbf{j} + (a_xb_y - a_yb_x)\mathbf{k}$$

により定める.

$$a_yb_z - a_zb_y = \begin{vmatrix} a_y & b_y \\ a_z & b_z \end{vmatrix},\ a_zb_x - a_xb_z = \begin{vmatrix} a_z & b_z \\ a_x & b_x \end{vmatrix},\ a_xb_y - a_yb_x = \begin{vmatrix} a_x & b_x \\ a_y & b_y \end{vmatrix}$$

なので,

$$\mathbf{a}\times\mathbf{b} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix}$$

と表すことも出来る.

定義より,

$$\begin{aligned} -2\mathbf{a}\cdot\mathbf{b} &= 2\mathrm{Re}(\mathbf{ab}) \\ &= \left(\mathbf{ab} + \overline{\mathbf{ab}}\right) \\ &= \mathbf{ab} + \mathbf{ba}. \end{aligned}$$

同様に,

$$2\mathbf{a}\times\mathbf{b} = 2\mathrm{Im}(\mathbf{ab}) = \mathbf{ab} - \mathbf{ba}. \tag{7.2}$$

内積の再確認をしよう.

命題 7.3.11 内積

$$\cdot : \mathbb{R}^3\times\mathbb{R}^3 \longrightarrow \mathbb{R};\quad (\mathbf{a},\mathbf{b}) \longmapsto \mathbf{a}\cdot\mathbf{b}$$

は正定値対称双線形形式である. すなわち次の満たす：

(1) $\mathbf{a}\cdot\mathbf{a} \geq 0$, 等号が成り立つ必要十分条件は $\mathbf{a} = \mathbf{0}$,

(2) $\mathbf{a}\cdot\mathbf{b} = \mathbf{b}\cdot\mathbf{a}$,

(3) $c\mathbf{a}\cdot\mathbf{b} = c(\mathbf{a}\cdot\mathbf{b})$,

(4) $(\mathbf{a}+\mathbf{a}')\cdot\mathbf{b} = \mathbf{a}\cdot\mathbf{b} + \mathbf{a}'\cdot\mathbf{a}$.

問 7.3.12 上の命題を確認せよ.

命題 7.3.13

$$\times : \mathbb{R}^3\times\mathbb{R}^3 \longrightarrow \mathbb{R}^3;\quad (\mathbf{a},\mathbf{b}) \longmapsto \mathbf{a}\times\mathbf{b}$$

は歪対称双線形射である. すなわち次の満たす：

(1) $\mathbf{a}\times\mathbf{b}=-\mathbf{b}\times\mathbf{a}$,

(2) $c\mathbf{a}\times\mathbf{b}=c(\mathbf{a}\times\mathbf{b})$,

(3) $(\mathbf{a}+\mathbf{a}')\times\mathbf{b}=\mathbf{a}\times\mathbf{b}+\mathbf{a}'\times\mathbf{a}$.

証明　(1) 式 (7.2) より, $2\mathbf{a}\times\mathbf{b}=\mathbf{ab}-\mathbf{ba}=-2\mathbf{b}\times\mathbf{a}$. (2),(3) も同様に示される. □

問 7.3.14

$$\det(\mathbf{a},\mathbf{b},\mathbf{c})=\mathbf{a}\cdot(\mathbf{b}\times\mathbf{c})$$

を示せ.

補題 7.3.15 $\mathbf{a}$ と $\mathbf{b}$ が一次従属ならば, $\mathbf{a}\times\mathbf{b}=\mathbf{0}$ である. $\mathbf{a}$ と $\mathbf{b}$ が一次独立ならば, $\mathbf{a}\times\mathbf{b}\neq\mathbf{0}$ であり,

$$\mathbf{a}\perp(\mathbf{a}\times\mathbf{b}),\quad \mathbf{b}\perp(\mathbf{a}\times\mathbf{b}).$$

問 7.3.16 補題を証明せよ.

ユークリッド線形空間の正規直交基底 $(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)$ は, $\det(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)=1$ を満たすとき, **右手系** と呼ばれる.

$\mathbf{a},\mathbf{b}$ が一次独立のとき, $\mathbf{a},\mathbf{b}$ の張る平面内に, 正規直交系 $\mathbf{e}_1,\mathbf{e}_2$ を次のようにとる：

$$\mathbf{a}=a\mathbf{e}_1,\quad \mathbf{b}=b(\cos\theta e_1+\sin\theta e_2)\quad (a,b>0,0<\theta<\pi).$$

次に, $(\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3)$ が右手系となるよう $\mathbf{e}_3$ をとる. このとき, 次が成り立つ：

補題 7.3.17 θ は, $\mathbf{a}$ と $\mathbf{b}$ のなす角であり,

$$\mathbf{a}\times\mathbf{b}=ab\sin\theta e_3=\|\mathbf{a}\|\cdot\|\mathbf{b}\|\sin\theta.$$

問 7.3.18 補題を証明せよ.

問 7.3.19 $(\mathbf{a},\mathbf{b})=(\mathbf{c},\mathbf{d})A\quad (A\in\mathrm{M}_2(\mathbb{R}))$ ならば,

$$\mathbf{a}\times\mathbf{b}=|A|\mathbf{c}\times\mathbf{d}$$

を示せ.

例題 7.3.20　（ベクトル三重積）

$$\mathbf{a}\times(\mathbf{b}\times\mathbf{c})=(\mathbf{a}\cdot\mathbf{c})\mathbf{b}-(\mathbf{a}\cdot\mathbf{b})\mathbf{c},$$

$$(\mathbf{a}\times\mathbf{b})\times\mathbf{c})=(\mathbf{b}\cdot\mathbf{c})\mathbf{a}-(\mathbf{a}\cdot\mathbf{b})\mathbf{c}.$$

（解） 各ベクトルの成分を書き表すことにより示されるが, ここでは, 四元数を利用して示す. 定義より,

$$\begin{aligned} 4\mathbf{a}\times(\mathbf{b}\times\mathbf{c}) &= \mathrm{Im}\,(\mathbf{a}\mathrm{Im}(\mathbf{bc})) \\ &= \mathrm{Im}\,(\mathbf{a}(\mathbf{bc}-\mathbf{cb})) \\ &= \mathbf{abc}-\mathbf{acb}+\mathbf{cba}-\mathbf{bca}. \end{aligned}$$

四元数環では積に関し結合法則が成り立つことに注意すると, 式 (7.1) より,

$$\begin{aligned} \mathbf{cba} &= \mathbf{c}(-\mathbf{ab}-2\mathbf{a}\cdot\mathbf{b}) \\ &= -(-2\mathbf{a}\cdot\mathbf{c}-\mathbf{ac})\mathbf{b}-2(\mathbf{a}\cdot\mathbf{b})\mathbf{c} \\ &= 2(\mathbf{a}\cdot\mathbf{c})\mathbf{b}+\mathbf{ac})\mathbf{b}-2(\mathbf{a}\cdot\mathbf{b})\mathbf{c}. \end{aligned}$$

同様に,

$$\mathbf{abc}=2(\mathbf{a}\cdot\mathbf{c})\mathbf{b}+\mathbf{bc})\mathbf{a}-2(\mathbf{a}\cdot\mathbf{b})\mathbf{c}.$$

従って, これら二式を, (7.3) に代入し, 最初の等式を得る. 二番目は, 最初の式から得られる. □

問 7.3.21 次の等式を示せ.

$$(\mathbf{a}\times\mathbf{b})\cdot(\mathbf{c}\times\mathbf{d})=\mathbf{a}\cdot\mathbf{c})(\mathbf{b}\cdot\mathbf{d})-(\mathbf{a}\cdot\mathbf{d})(\mathbf{b}\cdot\mathbf{b}).$$

最後に, 以前学んだ外積との関係を説明しよう. 単位行列 I_3 の三個の列ベクトルを $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ とする.

$$\mathbf{a}=a_1\mathbf{e}_1+a_2bfe_2+a_3\mathbf{e}_3,\mathbf{b}=b_1\mathbf{e}_1+b_2\mathbf{e}_2+b_3\mathbf{e}_3$$

に対し, $*$ を共役ベクトルをとる写像とすると,

$$\begin{aligned} *(\mathbf{a}\wedge\mathbf{b}) &= *((a_2b_3-a_3b_2)\mathbf{e}_2\wedge\mathbf{e}_3+(a_3b_1-a_1b_3)\mathbf{e}_3\wedge\mathbf{e}_1+(a_1b_2-a_2b_1)\mathbf{e}_1\wedge\mathbf{e}_2) \\ &= (a_2b_3-a_3b_2)\mathbf{e}_1+(a_3b_1-a_1b_3)\mathbf{e}_2+(a_1b_2-a_2b_1)\mathbf{e}_3 \\ &= \mathbf{a}\times\mathbf{b}. \end{aligned}$$

従って, 次を得る：

$$*(\mathbf{a}\wedge\mathbf{b})=\mathbf{a}\times\mathbf{b}.$$

付 録A　集合論

A.1　集合, 部分集合, 集合の演算

A.1.1　集合, 部分集合の定義

この節では, 集合に関する基礎的事項を説明する.

定義 A.1.1 数学的にはっきりした対象の集まりを**集合** という. 集合 X を構成している対象を X の **元**, あるいは **要素** という. x が X の元であるとき, X は x を含むともいい

$$x \in X \quad (\text{または } X \ni x)$$

と表す. y が集合 X に含まれない場合 $y \notin X$ と表す.

例 A.1.1 数の集合を次のように表す.

(1) $\mathbb{N}$：自然数 $1, 2, \cdots$ の全体の集合,

(2) $\mathbb{Z}$：整数 $\cdots, -2, -1, 0, 1, 2, \cdots$ の全体の集合,

(3) $\mathbb{Q}$：有理数全体の集合,

(4) $\mathbb{R}$：実数全体の集合,

(5) $\mathbb{C}$：複素数全体の集合.

集合は, 通常, { } を用いて記述する. 例えば $\{1, 2, 3\}$ は, 三個の自然数 $1, 2, 3$ からなる集合を表し, $\{\pm 1, \pm 3, \pm 5, \cdots\}$ は奇数全体の集合を表す. 対象 x に関する数学的にはっきりした条件 $C(x)$ に対し, $C(x)$ を満たす x の集合を

$$\{x \mid C(x)\}$$

と表す. x が集合 X の元で, 条件 $C(x)$ を満たすものを

$$\{x \in X \mid C(x)\}$$

と表す.

例 A.1.2 素数全体の集合は

$$\{p \mid p \text{ は素数 }\}$$

と表される.

$$\{1,2,3\} = \{\, x \in \mathbb{N} \mid 1 \le x \le 3\}, \quad \{\pm 1, \pm 3, \pm 5, \cdots\} = \{\, x \in \mathbb{Z} \mid x \text{ は奇数 }\}.$$

無理数の集合は

$$\{\, x \in \mathbb{R} \mid x \text{ は有理数ではない }\}$$

と表される.

定義 A.1.2 元を全く含まない集合も考えて, それを **空集合** といい,

$$\emptyset$$

で表す.

定義 A.1.3 X, Y を二つの集合とし,

$$x \in Y \quad \Longrightarrow \quad x \in X$$

が成り立つとき, Y は X の **部分集合** といい

$$Y \subset X \quad (\text{または } X \supset Y)$$

と表す. このとき Y **は** X **に含まれる**, 或いは, X **は** Y **を含む** ともいう.

二つの集合 X, Y に対し, $X \subset Y, Y \subset X$ が成り立つとき, X と Y は **等しい** といい, $X = Y$ と表す.

注意 A.1.1 $X \subset Y$ であり, $X \neq Y$ のとき, $X \subsetneq Y$ と表す.

$Y \subset X$ を $Y \subseteq X$ 或いは $Y \subseteqq X$ と書き, $Y \subsetneq X$ を $Y \subset$ と書くこともあるので, 他書を参照するときは, 注意を要する.

例 A.1.3 X, Y, Z を集合とする. この時, 次が成り立つ:

(1) $X \subset X$,

(2) $X \subset Y$ かつ $Y \subset Z \quad \Longrightarrow \quad X \subset Z$,

例題 A.1.4 空集合は, 任意の集合に含まれる. 逆に, 任意の集合に含まれる集合は空集合である.

（解） X を任意の集合とする. 定義より, $\emptyset \subset X$ を示すには,

$$x \in \emptyset \implies x \in X \tag{A.1}$$

を言えばよい. この命題は仮定が成立しない,

仮定が成り立たない命題は正しい

ので, 上記命題 (A.1) は正しい. よって $\emptyset \subset X$.

次に後半を示そう. 任意の集合に含まれる集合を A とする. 前半で示したことから, $\emptyset \subset A$ を得る. 一方, A の定め方から, $A \subset \emptyset$. 従って $A = \emptyset$. □

例題 A.1.5 空集合は唯一つである.

（解） $\emptyset'$ も空集合とすると $\emptyset' \subset \emptyset, \emptyset \subset \emptyset'$. 従って $\emptyset = \emptyset'$. □

例 A.1.4 集合 $X = \{1, 2, 3\}$ の部分集合は

$$\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{2, 3\},\ \{3, 1\},\ \{1, 2, 3\}$$

の 8 個である.

定義 A.1.6 X を集合とすると, $X, \emptyset$ は, X の部分集合である. X と異なる X の部分集合を **真部分集合** という.

定義 A.1.7 有限個の元からなる集合を **有限集合** といい, 有限集合でない集合を **無限集合** という. 有限集合 S に含まれる元の個数を $|S|$ または $\#S$ で表す. 空集合は有限集合とし, $|\emptyset| = 0$ とする.

例 A.1.5

$$|\{1, 2, 3, \cdots, n\}| = n.$$

次は, 明らかであろう.

補題 A.1.8 X, Y を有限集合とし, $|X| = |Y|$ とする. このとき, $X \subset Y$ ならば, $X = Y$ である.

注意 A.1.2 （Russell の逆理）

それ自身を元として含まない集合を **正常** 集合と名づける. すべての正常集合を集めたものを T としよう. 集合 T は自分自身を元として含むだろうか？

$T \notin T$ ならば, T の定義より $T \in T$. これは矛盾である.

$T \in T$ ならば, T の定義より $T \notin T$. これは矛盾である.

この不合理は, T を集合とすることに由来する. そこで, 正常集合の全体 T は集合ではないとする. しからば, 集合とは何かが問題となり, 集合論更には現代数学の根幹を揺るがし, 集合論の再構成が促された. これらについては, 程度を超えるので, 講義では取り扱わない.

A.1.2 和集合と共通部分

定義 A.1.9 二つの集合 X, Y に対し, 集合

$$X \cup Y := \{x \mid x \in X \text{ 又は } x \in Y\}$$

を X と Y との **和集合** という.

例 A.1.6

$$\{1, 2, 3\} \cup \{4, 5\} = \{1, 2, 3, 4, 5\}. \quad \{n \in\in \mathbb{R} | n \text{ は有理数 }\} \cup \{n \in\in \mathbb{R} | n \text{ は無理数 }\} = \mathbb{R}.$$

定義から, 直ちに, 次を得る：

補題 A.1.10 X, Y, Z を集合とする. このとき次が成り立つ.

(1) (冪等律) $X \cup X = X$,

(2) (交換律) $X \cup Y = Y \cup X$,

(3) (結合律) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$,

(4) $X \subset Y \iff X \cup Y = Y$,

(5) $X \cup \emptyset = X$.

補題 A.1.10 (3) の集合を $X \cup Y \cup Z$ と書き, X, Y, Z の和集合という. 四つ以上の場合も同様である.

定義 A.1.11 集合 X, Y に対し

$$X \cap Y := \{x \mid x \in X \text{ かつ } x \in Y\}$$

を X と Y との **共通部分** という. $X \cap Y \neq \emptyset, X \cap Y = \emptyset$ に従って, X と Y は **交わる**, **交わらない** という.

例 A.1.7

$$\{n \in\in \mathbb{Z} | n \text{ は } 3 \text{ の倍数 }\} \cup \{n \in \mathbb{Z} | n \text{ は } 5 \text{ の倍数 }\} = \{n \in \mathbb{Z} | n \text{ は } 15 \text{ の倍数 }\}.$$

定義から, 直ちに, 次を得る：

補題 A.1.12 X, Y, Z を集合とする. このとき次が成り立つ.

(1) (冪等律) $X \cap X = X$,

(2) (交換律) $X \cap Y = Y \cap X$,

(3) (結合律) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$,

(4) $X \subset Y \iff X \cap Y = X$,

(5) $X \cap \emptyset = \emptyset$.

補題 A.1.12 (3) の集合を $X \cap Y \cap Z$ と表し, X, Y, Z の共通部分という. 四つ以上の集合についても同様である.

問 A.1.13 A, B, X を集合 とする. このとき, 次を確かめよ.

(1) $A \subset X, B \subset X \implies A \cup B \subset X$.

(2) $X \subset A, X \subset B \implies X \subset A \cap B$.

(3) $A \subset B,\ \Longrightarrow\ X \cup A \subset X \cup B,\ X \cap A \subset X \cap B.$

命題 A.1.14 （分配律）X, Y, Z を集合とするとき, 次が成り立つ.

(1) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,

(2) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

証明 (1) $Y \cap Z \subset Y, Y \cap Z \subset Z$ なので,

$$X \cup (Y \cap Z) \subset X \cup Y, \quad X \cup (Y \cap Z) \subset X \cup Z.$$

従って

$$X \cup (Y \cap Z) \subset (X \cup Y) \cap (X \cup Z).$$

$a \in (X \cup Y) \cap (X \cup Z)$ を任意に取る. $a \in X$ ならば, $a \in X \cup (Y \cap Z)$. $a \notin X$ ならば, $a \in X \cup Y$ かつ $a \in X \cup Z$ なので $a \in Y \cap Z$. よって $a \in X \cup (Y \cap Z)$. 従って

$$X \cup (Y \cap Z) \supset (X \cup Y) \cap (X \cup Z).$$

(2) の証明は演習問題とする. □

問 A.1.15 命題 A.1.14 (2) を証明せよ.

問 A.1.16 A, B, C を有限集合とする. このとき次の等式を証明せよ.

(1) $|A \cup B| = |A| + |B| - |A \cap B|$,

(2) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$.

例 A.1.8 集合 X, Y に対し, $X - Y := \{x \in X \mid x \notin Y\}$ を **集合論的差** という. このとき, 次が成り立つ:

(1) $X \cap Y = \emptyset \quad \Longleftrightarrow \quad X - Y = X$.

(2) $X \subset Y \quad \Longleftrightarrow \quad X - Y = \emptyset$.

問 A.1.17 上の例を確かめよ.

定義 A.1.18 U を集合とし, X をその部分集合とする.

$$X^c := \{\, x \in U \mid x \notin X\} = U - X$$

を X の U に於ける **補集合** という.

定義より, 直ちに, 次が得られる：

命題 A.1.19 X, Y を集合 U の部分集合とする. このとき次が成り立つ:

(1) $(X^c)^c = X$,

(2) $\emptyset^c = U,\ U^c = \emptyset$,

(3) $U = X \cup X^c$,

(4) （**de Morgan の法則**）$(X \cup Y)^c = X^c \cap Y^c,\ (X \cap Y)^c = X^c \cup Y^c$.

問 A.1.20 上の命題を証明せよ.

例 A.1.9 X, Y を集合とする.

$$X \triangle Y := (X - Y) \cup (Y - X)$$

を X と Y との **対称差** という. このとき, 次が成り立つ:

(1) $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$,

(2) $X \triangle \emptyset = X$,

(3) $X \triangle X = \emptyset$,

(4) $X \triangle Y = Y \triangle X$,

(5) $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$.

問 A.1.21 上の例を確かめよ.

A.1.3 集合の直積

定義 A.1.22 n 個の集合 $X_1, \cdots, X_n$ に対し, 一番目に X_1 の元, 二番目に X_2 の元というように並べた n 個の元の列

$$(x_1, x_2, \cdots, x_n), \quad x_1 \in X_1, x_2 \in X_2, \cdots, x_n \in X_n$$

全体の集合を

$$X_1 \times X_2 \times \cdots \times X_n \quad \text{または} \quad \prod_{i=1}^{n} X_i$$

と表し, 集合 $X_1, X_2, \cdots, X_n$ の直積という. ただし, 順序の付いた二つの n 列

$$(x_1, x_2, \cdots, x_n), \quad (x'_1, x'_2, \cdots, x'_n)$$

が等しいとは,

$$x_1 = x'_1, x_2 = x'_2, \cdots, x_n = x'_n$$

が成り立つこととする.

特に $X_1 = X_2 = \cdots = X_n = X$ のとき, $X \times \cdots \times X$ を X^n とも表す.

例 A.1.10 $A=\{a_1,a_2,a_3\}, B=\{b_1,b_2\}$ のとき

$$A\times B=\{(a_1,b_1),(a_1,b_2),(a_2,b_1),(a_2,b_2),(a_3,b_1),(a_3,b_2)\},$$

$$B\times A=\{(b_1,a_1),(b_1,a_2),(b_1,a_3),(b_2,a_1),(b_2,a_2),(b_2,a_3)\},$$

$$A^2=A\times A=\{(a_1,a_1),(a_1,a_2),(a_1,a_3),(a_2,a_1),(a_2,a_2),(a_2,a_3),(a_3,a_1),(a_3,a_2),(a_3,a_3)\}.$$

例 A.1.11

$$X\times Y=\emptyset \iff X=\emptyset \text{ または } Y=\emptyset.$$

例 A.1.12 X,Y をそれぞれ n,m 個の元からなる有限集合とする. このとき $|X\times Y|=mn$.

例 A.1.13

$$X\subset X',\ Y\subset Y' \implies X\times Y\subset X'\times Y'.$$

例 A.1.14 $\mathbb{R}\times\mathbb{R}=\mathbb{R}^2$ を **座標平面** という.

例 A.1.15 座標平面 $\mathbb{R}^2$ の各点 (x,y) を複素数 $x+iy$ と見なすとき, 座標平面 $\mathbb{R}^2$ を **複素平面** という.

A.1.4 集合の分割と直和

定義 A.1.23 X を集合とし, $X_1,\cdots,X_n$ をその部分集合とする.

(1) $X_i\neq\emptyset$ $(i=1,\cdots,n)$,

(2) $X_i\cap X_j=\emptyset$ $(1\leq i<j\leq n)$,

(3) $X=X_1\cup\cdots\cup X_n$.

を満たすとき, $\{X_i\}_{i=1,\cdots,n}$ を, 集合 X の **分割** という.

例 A.1.16 無理数の集合を I と表すことにすれば, $\{\mathbb{Q},I\}$ は $\mathbb{R}$ の分割である.

例 A.1.17 5 で割ると余りが i である整数の集合を $[i]$ と表す：

$$[i]=\{5n+i\mid n\in\mathbb{Z}\}.$$

このとき, $\{[0],[1],[2],[3],[4]\}$ は, $\mathbb{Z}$ の分割である.

例 A.1.18

$$A=\{(x,y)\in\mathbb{R}^2\mid y>x\},\ B=\{(x,y)\in\mathbb{R}^2\mid y=x\},\ C=\{(x,y)\in\mathbb{R}^2\mid y<x\}$$

とするとき, $\{A,B,C\}$ は, 平面 $\mathbb{R}^2$ の分割である.

定義 A.1.24 $\{X_i\}_{i=1,\cdots,n}$ を集合とする. $X_i' = \{(x,i) \mid x \in X\}$ とし, これらの和集合

$$X_1' \cup X_2' \cup \cdots \cup X_n'$$

を

$$X_1 \coprod X_2 \coprod \cdots \coprod X_n$$

と表し, n 個の集合 $X_1, \cdots, X_n$ の **直和** という.

X_i が互いに他と交わらないときは, 単に, 和集合 $\cup_{i=1}^n X_i$ を

$$X_1 + \cdots + X_n$$

と表し, $X_1, \cdots, X_n$ の直和という.

例 A.1.19 $X_1 = \{1,2\}, X_2 = \{1,3,4\}$ のとき, これらの直和 $X_1 \coprod X_2$ は 5 個の元からなる集合であり, $X_1 \cup X_2$ は 4 個の元からなら集合である.

A.1.5 冪集合

定義 A.1.25 X を集合とするとき, X の部分集合全体のなす集合を, X の **冪集合** といい, $\mathcal{P}(X)$ と表す.

例 A.1.20 $\mathcal{P}(\emptyset) = \{\emptyset\}$ は 1 個の元 $\emptyset$ からなる集合である.

例 A.1.21 $X = \{1,2,3\}$ のとき,

$$\mathcal{P}(X) = \{\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{2,3\},\ \{3,1\},\ \{1,2,3\}\}.$$

問 A.1.26 X を n 個の元からなる集合とする. $|\mathcal{P}(X)| = 2^n$ を示せ.

問 A.1.27 X を n 個の元からなる集合とする. X の部分集合の組 (I,J) で $I \subset J$ を満たすものは何組あるか?

例 A.1.22 集合 X, Y に対し, 次が成り立つ:

$$X \subset Y \quad \Longleftrightarrow \quad \mathcal{P}(X) \subset \mathcal{P}(Y).$$

例題 A.1.28 X, Y を集合とする. このとき次が成り立つ.

(1) $\mathcal{P}(X \cap Y) = \mathcal{P}(X) \cap \mathcal{P}(Y)$,

(2) $\mathcal{P}(X \cup Y) \supset \mathcal{P}(X) \cup \mathcal{P}(Y)$. ここで等号は一般には成立しない.

(解) $X = \{1\}, Y = \{2\}$ とすると, $\mathcal{P}(X) = \{\emptyset, \{1\}\}, \mathcal{P}(Y) = \{\emptyset, \{2\}\}$ であり, $\mathcal{P}(X) \cup \mathcal{P}(Y) = \{\emptyset, \{1\}, \{2\}\}$. 一方 $X \cup Y = \{1,2\}$, 従って $\mathcal{P}(X \cup Y) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. よって $\mathcal{P}(X \cup Y) \supsetneq \mathcal{P}(X) \cup \mathcal{P}(Y)$. 他は省略. □

A.2 対応と写像

A.2.1 対応

集合 X, Y と, それらの直積 $X \times Y$ の部分集合 G との組 $\Gamma = (X, Y; G)$ を X から Y への対応という. X, Y をそれぞれ対応 Γ の **始集合**, **終集合** といい, G を Γ の **グラフ** という. X の部分集合 A に対し, Y の部分集合

$$\Gamma(A) := \{y \in Y \mid (x, y) \in G\ (\exists x \in A)\}$$

を Γ による A の **像** という. $x \in X$ に対し, $\Gamma(\{x\})$ を $\Gamma(x)$ と略記する. 特に, $A = X$ のとき, $\mathrm{Im}(\Gamma) := \Gamma(X)$ を Γ の像, または, **値域** という. Y の部分集合 B に対し, X の部分集合

$$\Gamma^{-1}(B) := \{x \in X \mid (x, y) \in G\ (\exists y \in B)\}$$

を Γ による B の **逆像** という. $y \in Y$ に対し, $\Gamma^{-1}(\{y\})$ を $\Gamma^{-1}(y)$ と略記する. 特に, $B = Y$ のとき,

$$\mathrm{Dom}(\Gamma) := \{x \in X \mid (x, y) \in G\ (\exists y \in Y)\}$$

を Γ の **定義域** という.

問 A.2.1

$$G = \{(x, y) \mid x = y^2\} \subset \mathbb{R} \times \mathbb{R}$$

とし, 対応 $\Gamma = (\mathbb{R}, \mathbb{R}; G)$ を考える. このとき, 次に答えよ.

(1) G を図示せよ.

(2) $\Gamma(-1), \Gamma(1), \Gamma([2, 4])$ を求めよ.

(3) $\mathrm{Dom}(\Gamma), \mathrm{Im}(\Gamma)$ を求めよ.

X, Y を集合とし, $\Gamma = (X, Y; G)$ を対応とする. 任意の $x \in \mathrm{Dom}\,\Gamma$ に対し, $|\Gamma(x)| = 1$ のとき, Γ は **一価** であるという. このとき, $\Gamma(x) = \{y\}$ のとき, $\Gamma(x) = y$ と表す.

問 A.2.2

$$G = \{(x, y) \mid y = \sin x\} \subset \mathbb{R} \times \mathbb{R}$$

とし, 対応 $\Gamma = (\mathbb{R}, \mathbb{R}; G)$ を考える. このとき, 次に答えよ.

(1) G を図示せよ.

(2) $\Gamma(-\pi), \Gamma(\pi/3), \Gamma([0, 2\pi])$ を求めよ.

(3) $\mathrm{Dom}(\Gamma), \mathrm{Im}(\Gamma)$ を求めよ.

(4) Γ は一価であることを確かめよ.

命題 A.2.3 $\Gamma = (X, Y; G)$ を集合の対応とし, A, A_1, A_2 は X の部分集合とするとき, 次が成り立つ:

(1) $A_1 \subset A_2 \Longrightarrow \Gamma(A_1) \subset \Gamma(A_2)$,

(2) $\Gamma(A_1 \cup A_2) = \Gamma(A_1) \cup \Gamma(A_2)$,

(3) $\Gamma(A_1 \cap A_2) \subset \Gamma(A_1) \cap \Gamma(A_2)$.

証明 (1) $y \in \Gamma(A_1)$ ならば, $(x, y) \in G$ $(\exists x \in A_1)$. $x \in A_2$ なので, $y \in \Gamma(A_2)$. (2) $y \in \Gamma(A_1 \cup A_2)$ ならば, $(x, y) \in G$ $(\exists x \in A_1 \cup A_2)$. $i = 1, 2$ に対し, $x \in A_i$ ならば, $y \in \Gamma(A_i)$ なので, $x \in \Gamma(A_1) \cup \Gamma(A_2)$. 逆に, $y \in \Gamma(A_1) \cup \Gamma(A_2)$ とする. $i = 1, 2$ に対し, $y \in \Gamma(A_i)$ ならば, $(x_i, y) \in G$ $(\exists x_i \in A_i)$. 従って, $y \in \Gamma(A_1 \cup A_2)$. (3) は演習問題とする. □

問 A.2.4 命題 **??** (3) を証明せよ.

X から Y への対応 $\Gamma = (X, Y; G)$ に対し,

$$\Gamma^{-1} = (Y, X; {}^t G), \quad {}^t G = \{(y, x) \mid (x, y) \in G\}$$

とする. このとき対応 Γ^{-1} を Γ の **逆対応** という.

Y の部分集合 B の Γ^{-1} による像は, Γ による逆像と一致する：

$$\begin{aligned} \Gamma^{-1}(B) &= \{x \in X \mid (y, x) \in {}^t G \ (\exists y \in B)\} \\ &= \{x \in X \mid (x, y) \in G \ (\exists y \in B)\}. \end{aligned}$$

明らかに,

$$\mathrm{Dom}(\Gamma^{-1}) = \mathrm{Im}(\Gamma), \quad \mathrm{Im}(\Gamma^{-1}) = \mathrm{Dom}(\Gamma), \quad (\Gamma^{-1})^{-1} = \Gamma$$

が成り立つ.

命題 A.2.5 $\Gamma = (X, Y; G)$ を集合の対応とする.

(1) $A \subset \mathrm{Dom}\,\Gamma$ ならば, $\Gamma^{-1}(\Gamma(A)) \supset A$.

(2) $B \subset \mathrm{Im}\,\Gamma$ ならば, $\Gamma(\Gamma^{-1}(B)) \supset B$.

証明 (1) $a \in A$ とすると, $A \subset \mathrm{Dom}\,\Gamma$ より, $(a, y) \in G$ $(\exists y \in Y)$. このとき, $y \in \Gamma(A)$ であり, $a \in \Gamma^{-1}(\Gamma(A))$. (2) は (1) に於いて, Γ, A を Γ^{-1}, B に置き換えると得られる. □

A.2.2 写像とそのグラフ

X, Y を集合とする. 定義域が始集合に一致する一価対応 $f = (X, Y; G)$ を, X から Y への **写像** または **関数** といい,

$$f : X \longrightarrow Y, \quad X \xrightarrow{f} Y$$

と表す. $G_f := G$ を写像 f のグラフという. $X = \mathrm{Dom}\, f$ であり, 一価なので, **任意の** $x \in X$ **に対し,** $y = f(x) \in Y$ **が唯一つ定まる**. f による x の像が y であることを $x \mapsto y$ と表すこともある.

問 A.2.6 写像 $f : X \longrightarrow Y$ のグラフは

$$G_f = \{(x, f(x)) \mid x \in X\}$$

であることを確かめよ.

問 A.2.7 二つの写像 $f : X \longrightarrow Y$, $g : U \longrightarrow V$ が等しい為の必要十分条件は

$$X = U, \quad Y = V, \quad f(x) = g(x) \ \ (\forall x \in X)$$

であることを確かめよ

例 A.2.1 集合 X の各元 x に対し, $x \in X$ を対応させる写像を **恒等写像** といい,

$$I_X : X \longrightarrow X$$

と表す. I_X のグラフは, X の **対角線集合**

$$\Delta_X = \{(x, x) \mid x \in X\}$$

となる.

例 A.2.2 X, Y を集合とし, $y_0 \in Y$ とする. X の各元 $x \in X$ に $y_0 \in Y$ を対応させる写像 $f : X \longrightarrow Y$ を **定値写像** または **定数関数** という. f のグラフは

$$X \times \{y_0\}$$

である.

例 A.2.3 集合 X から実数全体の集合 $\mathbb{R}$, または複素数全体の集合 $\mathbb{C}$ への写像を, それぞれ X で定義された, 或いは, X 上の **実数値関数**, **複素数値関数**という.

例 A.2.4 写像 f, g を次のように定める:

$$\begin{aligned} f &: \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto \sin(2x), \\ g &: \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto 2\sin(x)\cos(x). \end{aligned}$$

このとき, $f = g$ である.

X から Y への写像全体のなす集合を $\mathrm{Map}(X, Y)$ と表す.

注意 A.2.1 任意の集合 Y に対し, $\emptyset \times Y = \emptyset$ なので, 空集合 $\emptyset$ から集合 Y への対応は

$$\emptyset_Y = (\emptyset, Y; \emptyset)$$

に限り, これは写像である.

また, 任意の集合 X に対し, 集合 X から $\emptyset$ への対応も

$$(X, \emptyset; \emptyset)$$

に限る. これが写像になるのは, $X = \emptyset$ となるときに限り, $\emptyset_\emptyset$ である.

定義 A.2.8 集合 X から実数全体の集合 $\mathbb{R}$, または複素数全体の集合 $\mathbb{C}$ への写像を **関数** という. それぞれ X で定義された, 或いは, X 上の **実数値関数**, **複素数値関数**という.

例 A.2.5 $f : X\rangle Y$ を集合 X から集合 Y への写像とする. X の部分集合 S から Y への写像

$$f|_S : S \longrightarrow Y$$

を $f|_S(s) = f(s), \forall s \in S$ により定め, 写像 f の S への **制限** という.

例 A.2.6 X を集合とする. $X \times X$ から X への写像を X 上の **二項演算** という. 例えば, 二つの整数に対し, それらの和, 積を対応させる写像

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a, b) \longmapsto a + b, \quad \times : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a, b) \longmapsto ab$$

は, 加法, 乗法と呼ばれる $\mathbb{Z}$ 上の二項演算である.

A.2.3 写像による像と逆像

$f : X \longrightarrow Y$ を集合の写像とし, G_f をそのグラフとする. 集合の写像を **集合射** と短くいうこともある.

X の部分集合 S に対し, f による S の像は

$$f(S) = \{f(s) \mid s \in S\}$$

である. また, f の像は $\mathrm{Im}(f) = f(X)$ となる.

一方, Y の部分集合 T に対し, f による T の逆像は

$$f^{-1}(T) = \{x \in X | f(x) \in T\}$$

である. 定義から, $x \in X$ に対し

$$x \in f^{-1}(T) \quad \Longleftrightarrow \quad f(x) \in T \tag{A.2}$$

が成り立つ. $f^{-1}(\{y\})$ を, 単に, $f^{-1}(y)$ と表す. [1]

問 A.2.9 $f : X \longrightarrow Y$ を集合射とし, S_1, S_2 は X の部分集合とするとき,

$$f(S_1 \cap S_2) \subset f(S_1) \cap f(S_2)$$

を示せ. また, 等号が成立しない例を挙げよ.

定義から, 次を得る：

問 A.2.10 $f : X \longrightarrow Y$ を集合射とし, T, T_1, T_2 を Y の部分集合とする. このとき次が成り立つことを証明せよ：

[1] 後に学ぶ逆写像と混同しないよう注意せよ.

(1) $T_1 \subset T_2 \Longrightarrow f^{-1}(T_1) \subset f^{-1}(T_2)$,

(2) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$,

(3) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$.

例 A.2.7 $f^{-1}(T) = \emptyset$ だからといって, $T = \emptyset$ とは限らない. 例えば, 写像 $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin(x)$ と, $T = [2, 3] \subseteq \mathbb{R}$ に対し, $f^{-1}(T) = \emptyset$.

命題 A.2.11 $f : X \longrightarrow Y$ を集合射とするとき, 次が成り立つ.

(1) $S \subset X \implies f^{-1}(f(S)) \supset S$.

(2) $T \subset Y \implies f(f^{-1}(T)) \subset T$.

(3) $T \subset \mathrm{Im}(f) \implies f(f^{-1}(T)) = T$.

(4) $S \subset X \implies f(X - S) \supset f(X) - f(S)$.

(5) $T \subset Y \implies f^{-1}(Y - T) = X - f^{-1}(T)$.

(6) $f^{-1}(Y) = X$.

証明 (1) 任意の $s \in S$ に対し, $f(s) \in f(S)$. 従って, 式 (A.2) により, $s \in f^{-1}(f(S))$.
(2) $f(x) \in f(f^{-1}(T))$ $(x \in f^{-1}(T))$ を任意にとると, 式 (A.2) により, $f(x) \in T$.
(3) $f(f^{-1}(T) \subset T$ は, 2. で示されている. 従って, 逆の包含関係を示せばよい. 任意に $t \in T$ をとる. 仮定により, $t = f(x)$ $(\exists x \in X)$ と表される. 式 (A.2) により, $x \in f^{-1}(T)$. 従って $t = f(x) \in f(f^{-1}(T))$ となり, $T \subset f(f^{-1}(T))$.
(4) 任意の $y \in f(X) - f(S)$ をとると, $y = f(x)$ $(x \in X - S)$ と表される. すなわち $y \in f(X - S)$.
(5) 任意に $x \in f^{-1}(Y - T)$ をとると, 式 (A.2) により, $f(x) \in Y - T$. 特に, $f(x) \notin T$. 再び, 式 (A.2) により, $x \notin f^{-1}(T)$ 従って $x \in X - f^{-1}(T)$. 逆に, 任意に $x \in X - f^{-1}(T)$ をとれば, $x \notin f^{-1}(T)$. 従って $f(x) \notin T$ であり, $f(x) \in Y - T$. 式 (A.2) により, $x \in f^{-1}(Y - T)$.
(6) 任意に $x \in X$ をとれば, $f(x) \in Y$. 従って $x \in f^{-1}(Y)$ となり, $X \subset f^{-1}(Y)$. 逆の包含関係は明らかである. □

例 A.2.8 写像 $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto x^2$ を考える. 閉区間 $[0, 2]$ を S とするとき, $f(S) = [0, 4]$, $f^{-1}(f(S)) = [-2, 2]$ となり, これは, S を真に含む.

また, $T = [-1, 2]$ とすれば, $f^{-1}(T) = [0, \sqrt{2}]$, $f(f^{-1}(T)) = [0, 2]$ で, これは T に, 真に含まれる.

以上により, 命題 A.2.11 の, (1), (2) において, 等号は, 一般には, 成り立たないことがわかる.

A.2.4 写像の合成

定義 A.2.12 $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ を集合射とする.

$$g \circ f : X \longrightarrow Z, \quad (g \circ f)(x) = g(f(x)), \forall x \in X$$

により定められる写像を f と g との **合成写像** または **合成射** という.

例 A.2.9 二つの写像

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto \cos(x), \quad g : \mathbb{R} \longrightarrow \mathbb{R}, \quad y \longrightarrow y^3$$

に対し

$$g \circ f : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto (\cos(x))^3 = \cos^3(x), \quad f \circ g : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto \cos(x^3).$$

命題 A.2.13 $f : X \longrightarrow Y, g : Y \longrightarrow Z, h : Z \longrightarrow U$ を集合射とする. このとき, 次が成り立つ:

(1) $h \circ (g \circ f) = (h \circ g) \circ f$,

(2) $I_Y \circ f = f$, $f \circ I_X = f$.

証明 (1) 任意の $x \in X$ に対し,

$$(h \circ (g \circ f))(x) = h(g \circ f)(x)) = h((g(f(x))) = ((h \circ g) \circ f)(x).$$

従って, 定義 A.2.7 により, $h \circ (g \circ f) = (h \circ g) \circ f$. (2) は恒等写像の定義から, 直ちに得られる. □

例 A.2.10 X を集合とし, X から X への写像全体の集合を $\mathrm{Map}(X)$ と表す. このとき,

$$\circ : \mathrm{Map}(X) \times \mathrm{Map}(X) \longrightarrow \mathrm{F}(X), \quad (f, g) \longmapsto f \circ g$$

は, $\mathrm{Map}(X)$ 上の演算である. この演算は結合法則, すなわち,

$$h \circ (g \circ f) = (h \circ g) \circ f \quad (\forall f, g, h \in \mathrm{F}(X))$$

を満たす. 更に,

$$I_X \circ f = f \circ I_X = f \qquad (\forall f \in \mathrm{Map}(X))$$

を満たす.

問 A.2.14 上の例を確かめよ.

A.2.5 全射, 単射, 全単射

$f : X \longrightarrow Y$ を集合 X から集合 Y への写像とする.

(1) $\mathrm{Im}(f) = f(X) = Y$ となるとき, f を **全射**, または **上への写像** という.

(2) $f(x) = f(x') \Longrightarrow x = x'$ が成り立つとき, f を **単射**, または **１対１の写像** という.

(3) 単射かつ全射である写像を **全単射**, または **１対１上への写像** という.

$f(X) \subseteq Y$ なので, f が全射であるための条件は, $f(X) \supset Y$ であり, 即ち,

$$f^{-1}(y) \neq \emptyset \quad (\forall y \in Y)$$

が成り立つことである.

また, f が単射であるための条件は,

$$x \neq x' \Longrightarrow f(x) \neq f(x')$$

といってもよいし, 更に,

$$|f^{-1}(y)| = 1 \quad (\forall y \in \mathrm{Im}(f))$$

といってもよい.

例 A.2.11 0 以上の実数の集合を $\mathbb{R}_{\geq 0}$ で表す. 写像

$$f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}, \quad x \longmapsto x^2$$

は全射だが単射ではない. しかし f の $\mathbb{R}_{\geq 0}$ への制限

$$f|_{\mathbb{R}_{\geq 0}} : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$$

は全単射である.

例 A.2.12 $\mathbb{R}$ から $\mathbb{R}$ への 3 次関数は全射である.

例 A.2.13 写像

$$f : \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}, \quad x \longmapsto (x, x^3)$$

は単射であるが, 全射ではない.

例 A.2.14 X を集合 Y の部分集合とする. 写像

$$\iota : X \longrightarrow Y, \quad x \longmapsto x$$

は単射である. これを **自然な単射** という.

例 A.2.15 $X_1, \cdots, X_n$ を空でない集合とし, $i \in \{1, 2, \cdots, n\}$ とする. 各 $(x_1, \cdots, x_n) \in X_1 \times \cdots \times X_n$ に対し x_i を対応させる写像

$$pr_i : X_1 \times \cdots \times X_n \longrightarrow X_i$$

は全射であり, i 番目への **射影** という.

例 A.2.16 集合 X の恒等写像 $I_X : X \longrightarrow X$ は全単射である.

定義 A.2.15 X の部分集合 $A \subseteq X$, すなわち, $\mathcal{P}(X)$ の元 A に対し

$$\chi_A(x) = \begin{cases} 1 & (x \in A) \\ 0 & (x \in X - A) \end{cases}$$

とすると, $\chi_A \in \mathrm{Map}(X, \{0, 1\})$ であり, A の （X に於ける） **定義関数**, または, **特徴関数** という.

命題 A.2.16 X を集合とする．このとき

$$\chi : \mathcal{P}(X) \longrightarrow \mathrm{Map}(X, \{0,1\}), \quad A \longmapsto \chi_A$$

は全単射であり，

$$\mathrm{Map}(X, \{0,1\}) \simeq \mathcal{P}(X).$$

証明 $\chi(A) = \chi_A = \chi_B = \chi(B)$ とすると

$$A = \{x \in X \mid \chi_A(x) = 1\} = \{x \in X \mid \chi_B(x) = 1\} = B.$$

従って, χ は単射である．また, 任意の $f \in \mathrm{Map}(X, \{0,1\})$ に対し

$$A := \{x \in X \mid f(x) = 1\}$$

とすれば, $\chi(A) = \chi_A = f$ となり, χ は全射である． □

命題 A.2.17 $f : X \longrightarrow Y$ を集合射とし，$S, S_1, S_2 \subset X, T \subset Y$ とする．このとき次が成り立つ．

(1) f が単射ならば $f^{-1}(f(S)) = S$.

(2) f が全射ならば $f(f^{-1}(T)) = T$.

(3) f が単射ならば $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$.

証明 (1) 命題 A.2.11 (1) を考慮すれば, $S \supset f^{-1}(f(S))$ を示せばよい．任意に $s \in f^{-1}(f(S))$ をとる．式 (A.2) により, $f(s) \in f(S)$. 従って $f(s) = f(s')$ となる $s' \in S$ が存在する．f は単射なので, $s = s' \in S$.
(2) (1) と同様に, $T \subset f(f^{-1}(T))$ を示せばよい． 任意に $t \in T$ をとると, f は全射なので $t = f(x)$ $(\exists x \in X)$ と表される．式 (A.2) により, $x \in f^{-1}(T)$. 従って, $t = f(x) \in f(f^{-1}(T))$.
(3) 問 A.2.9 を考慮すれば, $f(S_1) \cap f(S_2) \subset f(S_1 \cap S_2)$ を示せばよい．任意に $y \in f(S_1) \cap f(S_2)$ をとると, $y = f(s_1) = f(s_2)$ $(s_1 \in S_1, s_2 \in S_2)$ と表される．f は単射なので $s_1 = s_2 \in S_1 \cap S_2$. 従って $y = f(s_1) = f(s_2) \in f(S_1 \cap S_2)$. □

命題 A.2.18 $f : X \to Y$ を有限集合 X から有限集合 Y への写像とし, $|X| = |Y|$ とする．このとき次は同値である．

(1) f は単射である．

(2) f は全射である．

(3) f は全単射である．

この命題は, 次の例を考えれば, 当然のことと認識される．

例 A.2.17 X をりんご 5 個の集合とし, Y を 5 人の子供の集合とする．各りんごを子供に配る写像 f を考える．このとき次は同値である．

(1) 1個ずつ配る. すなわち f は単射.

(2) 全員に配る. すなわち f は全射.

(3) 1個ずつ全員に配る. すなわち f は全単射.

命題 A.2.19 $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ を集合の写像とする. このとき次が成り立つ.

(1) f, g が単射ならば $g \circ f$ も単射である.

(2) f, g が全射ならば $g \circ f$ も全射である.

(3) f, g が全単射ならば $g \circ f$ も全単射である.

(4) $g \circ f$ が単射ならば f は単射である.

(5) $g \circ f$ が全射ならば g は全射である.

証明 (1). $x, x' \in X$ に対し, $(g \circ f)(x) = (g \circ f)(x')$ とする. 従って $g(f(x)) = g(f(x'))$. g が単射なので, $f(x) = f(x')$. f が単射なので, $x = x'$. よって $g \circ f$ は単射である.
(2). f が全射なので $f(X) = Y$. g が全射なので, $g(Y) = Z$. 従って, $(g \circ f)(X) = g(f(X)) = g(Y) = Z$ となり, $g \circ f$ は全射である.
(3). (1) と (2) を組み合わせて (3) を得る.
(4). $x, x' \in X$ に対し $f(x) = f(x')$ とする. このとき, $g(f(x)) = g(f(x'))$. $g \circ f$ が単射なので, $x = x'$. 従って f は単射である.
(5). $g(Y) = Z$ を示せばよい. $g(Y) \subseteq Z$ は明らかなので, $g(Y) \supset Z$ を示す. 任意の $z \in Z$ をとる. $g \circ f$ が全射なので $g(f(x)) = z$ となる $x \in X$ が存在する. $f(x) \in Y$ なので, $z = g(f(x)) \in g(Y)$.
□

例題 A.2.20 $f : X \longrightarrow Y$ を集合 X から集合 Y への全射とする. $g, Y \longrightarrow Z$, $g' : Y \longrightarrow Z$ を集合 Y から集合 Z への二つの写像で $g \circ f = g' \circ f$ を満たすとする. このとき $g = g'$ である.

証明 任意に $y \in Y$ をとる. f は全射なので, $f(x) = y$ となる $x \in X$ が存在する. このとき, $g(y) = g(f(x)) = g'(f(x)) = g'(y)$. y は任意なので $g = g'$. □

命題 A.2.21 X, Y, Z を集合とする. このとき, 次が成り立つ:

(1) $\mathrm{Map}(X \times Y, Z) \simeq \mathrm{Map}(X, \mathrm{Map}(Y, Z))$.

(2) $\mathrm{Map}(X, Y) \times \mathrm{Map}(X, Z) \simeq \mathrm{Map}(X, Y \times Z)$.

(3) $\mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z) \simeq \mathrm{Map}(X + Y, Z)$.

証明 (1). 写像

$$\Phi : \mathrm{Map}(X \times Y, Z) \longrightarrow \mathrm{Map}(X, \mathrm{Map}(Y, Z)),\ f \longmapsto f_x : y \longmapsto f(x, y)$$

が全単射であることを示す. $\Phi(f)=\Phi(g)$ とする. 任意の $(x,y)\in X\times Y$ に対し,

$$\Phi(f)(x):y\longmapsto f(x,y),\quad \Phi(g)(x):y\longmapsto g(x,y)$$

従って $f=g$ となり, Φ は単射. 逆に, 任意の $\xi\in \mathrm{Map}(X,\mathrm{Map}(Y,Z))$ をとる. $x\in X, y\in Y$ に対し, $\xi(x)(y)=f(x,y)$ とすると, $f\in \mathrm{Map}(X\times Y,Z)$ であり, $\Phi(f)=\xi$. 従って, Φ は全射.
(2). 写像

$$\Psi:\mathrm{Map}(X,Y)\times\mathrm{Map}(X,Z)\longrightarrow \mathrm{Map}(X,Y\times Z)),\ (f,g)\longmapsto [x\longmapsto (f(x),g(y))]$$

が全単射であることが容易に示される.
(3). $X\cap Y=\emptyset$ と仮定する. 写像

$$\Xi:\mathrm{Map}(X,Z)\times\mathrm{Map}(Y,Z)\longrightarrow \mathrm{Map}(X+Y,Z),\ (f,g)\longmapsto \Xi(f,g)$$

が全単射であることは容易に示される. ただし, $\Xi(f,g)$ は, $x\in X$ ならば, $\Xi(f,g)(x)=f(x)$, $y\in Y$ ならば, $\Xi(f,g)(y)=g(y)$ で定義される写像である.
$X\cap Y\neq\emptyset$ の場合は演習問題とする. □

問 A.2.22 $X\cap Y\neq\emptyset$ の場合に, 命題 *syazoukuukan* (3) を証明せよ.

例 A.2.18 $X_1,\cdots,X_n$ を n 個の集合とする. $I=\{1,\cdots,n\}$ とし,

$$\mathcal{M}=\{f:I\longrightarrow X_1\cup\cdots\cup X_n\mid f(i)\in X_i\ (\forall i\in I)\}$$

とする. このとき

$$\mathcal{M}\longrightarrow X_1\times\cdots X_n,\quad f\longmapsto (f(1),\cdots,f(n))$$

は全単射である. 即ち, 集合の直積 $X_1\times\cdots\times X_n$ と写像の集合 $\mathcal{M}$ が同一視される.

問 A.2.23 上の例を確かめよ.

A.2.6 逆写像

命題 A.2.24 $f:X\longrightarrow Y$ を集合射とし, G_f をそのグラフとする. 対応 $f=(X,Y;G_f)$ の逆対応 $f^{-1}=(Y,X;{}^tG_f)$ が写像になる為の必要十分条件は f が全単射となることである.

証明 f^{-1} は写像とする. このとき, $\mathrm{Dom}(f^{-1})=\mathrm{Im}(f)=Y$ であり, $|f^{-1}(y)|=1\ (\forall y\in Y)$. 従って, f は全射であり, 単射である. この証明を, 逆に辿れば, 十分性を得る. □

$f:X\longrightarrow Y$ を全単射とする. このとき, Y の各元 y に $x=f^{-1}(y)$ を対応させる写像を $f^{-1}:Y\longrightarrow X$ と表し, f の **逆写像** という:

$$f^{-1}:Y\longrightarrow X;\quad y\longmapsto x.$$

このとき逆写像も全単射であり

$$(f^{-1})^{-1}=f,\quad f\circ f^{-1}=I_Y,\quad f^{-1}\circ f=I_X \tag{A.3}$$

が成り立つ.

注意 A.2.2 $y \in Y$ の逆像 $f^{-}(\{y\}) = \{x\}$ は X の部分集合であり, 逆写像 f^{-1} による y の像 $f^{-1}(y)$ は, X の元である. しかし, わざと混同して, $f^{-1}(\{y\})$ を $f^{-1}(y)$ と表したし, f^{-1} が一価ならば, $f^{-1}(y) = x$ と表した.

例 A.2.19 $X = \{1, 2, 3\}$ から $Y = \{a, b, c\}$ への写像 f を

$$f(1) = c,\ f(2) = b,\ f(3) = a$$

により定める. このとき, f は全単射であり, その逆写像 $f^{-1} : Y \longrightarrow X$ は

$$f^{-1}(a) = 3,\ f^{-1}(b) = 2,\ f^{-1}(c) = 1$$

を満たす.

例 A.2.20 写像

$$\mathrm{Tan} : (-\frac{\pi}{2}, \frac{\pi}{2}) \longrightarrow \mathbb{R}, \quad x \longmapsto \tan(x)$$

は全単射であり, その逆写像を Tan^{-1} と表す:

$$\mathrm{Tan} : \mathbb{R} \longrightarrow (-\frac{\pi}{2}, \frac{\pi}{2}), \quad \alpha \longmapsto x\ (\tan(x = \alpha).$$

例 A.2.21 正の実数全体の集合を $\mathbb{R}_{>0}$ と表す. a を正の実数とするとき指数関数

$$f : \mathbb{R} \longrightarrow \mathbb{R}_{>0}, \quad f(x) = a^x$$

は全単射であり, その逆写像は a を底とする対数関数

$$g : \mathbb{R}_{>0} \longrightarrow \mathbb{R}, \quad g(y) = \log_a(y)$$

である.

集合の写像 $f : X \longrightarrow Y$ に対し, 写像 $g : Y \longrightarrow X$ が存在し,

$$g \circ f = id_X, \quad f \circ g = id_Y$$

を満たすとき, f を **同型射** という.

集合 X から集合 Y への同型射が存在するとき, X と Y は **対等** または **同型** であるといい

$$X \simeq Y$$

と表す.

命題 A.2.25 集合の写像 $f : X \longrightarrow Y$ に対し, 次は同値である：

(1) f は同型射である,

(2) f は全単射である.

証明 (1) $\Longrightarrow$ (2) f を同型射とすると, $g \circ f = id_X, \quad f \circ g = id_Y$ を満たす写像 $g : Y \longrightarrow X$ が存在する. id_X, id_Y は全単射なので, 命題 A.2.19 (4), (5) により, f, g は共に全単射である. また, $g \circ g^{-1} = id_X, f \circ f^{-1} = id_Y$ なので, 例 A.2.20 により, $f = g^{-1}, g = f^{-1}$ を得る. (2) $\Longrightarrow$ (1) f を全単射とし, その逆写像を f^{-1} とする. このとき, $f^{-1} \circ f = id_X, \quad f \circ f^{-1} = id_Y$ を満たすので, f は同型射である. □

命題 A.2.26 X, Y, Z を集合とする. このとき次が成り立つ.

(1) $X \simeq X$.

(2) $X \simeq Y \implies Y \simeq X$.

(3) $X \simeq Y, Y \simeq Z \implies X \simeq Z$.

証明 (1). 恒等写像 $id_X : X \longrightarrow X$ は全単射なので, $X \simeq X$. (2). $X \simeq Y$ なので, 全単射 $f : X \longrightarrow Y$ が存在する. このとき, f の逆写像 $f^{-1} : Y \longrightarrow X$ も全単射なので, $Y \simeq X$. (3). 仮定により, 全単射 $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ が存在する. 命題 A.2.19 (3) により, 合成写像 $g \circ f : X \longrightarrow Z$ も全単射である. 従って $X \simeq Z$. □

例 A.2.22 X を集合とし, X から X への全単射の全体を $\mathrm{Sym}(X)$ と表す. 写像の合成が定める $\mathrm{Map}(X)$ 上の二項演算は, $\mathrm{Sym}(X)$ 上の二項演算を導く：

$$\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \longrightarrow \mathrm{Sym}(X).$$

$\circ$ は次を満たす：

(1) $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu) \quad (\forall \sigma, \tau, \mu \in \mathrm{Sym}(X))$.

(2) $I_X \circ \sigma = \sigma \circ I_X = \sigma \quad (\forall \sigma \in \mathrm{Sym}(X))$.

(3) $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = I_X \quad (\forall \sigma \in \mathrm{Sym}(X))$.

問 A.2.27 上の例を確かめよ.

A.3 添数付けられた族と選出公理

A.3.1 添数付けられた族

I を空でない集合とする. このとき, I の各元 i に対し, 集合 X の元が与えられること, また, I の各元 i に対し, 集合 X_i が与えられることを, もう少し正確に述べよう.

各自然数 n に実数 a_n が与えられることは, 写像

$$\mathbb{N} \longrightarrow \mathbb{R}, \qquad n \longmapsto a_n$$

が与えられることに他ならない. この考えを一般化する.

空でない集合 I から集合 X への写像

$$I \longrightarrow X, \quad i \longmapsto x_i$$

を I により **添数付けられた** X の **元の族** といい, I を **添数集合**, I の元を **添数** という. この元の族を

$$(x_i)_{i\in I}$$

と表す.

また, 空でない集合 I から, 集合を要素とする集合 $\mathcal{X}$ への写像

$$I \longrightarrow \mathcal{X}, \quad i \longmapsto X_i$$

を, 添数集合 I により添数付けられた **集合族** といい

$$(X_i)_{i\in I}$$

と表す.

例 A.3.1 空でない集合 I から, 集合 X の冪集合 $\mathcal{P}(X)$ への写像

$$I \longrightarrow \mathcal{P}(X); \quad i \longmapsto X_i$$

を I により添数付けられた X の **部分集合族** といい, 同じく, $(X_i)_{i\in I}$ と表す.

I を添数集合とする集合族 $(X_i)_{i\in I}$ に対し,

$$\bigcup_{i\in I} X_i := \{x \mid x \in X_i \ (\exists i \in I)\}, \quad \bigcap_{i\in I} X_i := \{x \mid x \in X_i \ (\forall i \in I)\}$$

を, 集合族 $(X_i)_{i\in I}$ の **和集合**, **共通部分** という.

注意 A.3.1 I により添数付けられた集合族 $(X_i)_{i\in I}$ に対し,

$$X = \bigcup_{i\in I} X_i$$

とすると, $(X_i)_{i\in I}$ は, X の部分集合族と見なされる.

以後, 特に断らない限り, 集合族 $(X_i)_{i\in I}$ は, 或る集合 X の部分集合族とする.

例 A.3.2 自然数 n に対し, $X_n := [0, \frac{1}{n}]$ とする. このとき,

$$\mathbb{N} \longrightarrow \mathcal{P}(\mathbb{R}), \quad n \longmapsto X_n$$

は $\mathbb{N}$ を添数集合とする集合族 $(X_n)_{n\in\mathbb{N}}$ である.

例 A.3.3 例 A.3.2 の集合族 $(X_n)_{n\in\mathbb{N}}$ に対し

$$\bigcup_{n\in\mathbb{N}} X_n = [0,1], \quad \bigcap_{n\in\mathbb{N}} X_n = \{0\}.$$

例 A.3.4 集合族 $(X_n)_{n\in\mathbb{N}}$ に対し, $\cup_{n\in\mathbb{N}}X_n, \cap_{n\in\mathbb{N}}X_n$ を

$$\bigcup_{n=1}^{\infty} X_n, \quad X_1 \cup X_2 \cup \cdots, \qquad \bigcap_{n=1}^{\infty} X_n, \quad X_1 \cap X_2 \cap \cdots$$

と表すこともある. また, $I = \{1, 2, \cdots, n\}$ の場合, $\cup_{i\in I}X_i, \cap_{i\in I}X_i$ を

$$\bigcup_{i=1}^{n} X_i, \quad X_1 \cup \cdots \cup X_n, \qquad \bigcap_{i=1}^{n} X_i, \quad X_1 \cap \cdots \cap X_n$$

と表すこともある.

例 A.3.5 X, Y の部分集合族 $(X_i)_{i\in I}, (Y_j)_{j\in J}$ に対し, $(X_i \times Y_j)_{(i,j)\in I\times J}$ は, $X \times Y$ の部分集合族である.

A.3.2 選出公理と集合族の直積

I を空でない集合とする. 任意の $i \in I$ に対し $X_i \neq \emptyset$ を満たす集合族 $(X_i)_{i\in I}$ を **正規集合族** という.

(選出公理) I を空でない集合とし, $(X_i)_{i\in I}$ を, X の部分正規集合族とする. このとき, 写像 $c : I \longrightarrow X$ で $c(i) \in X_i$ $(\forall i \in I)$ を満たすものが存在する.

X の元の族 c を, 集合族 $(X_i)_{i\in I}$ の, **選出関数** という.

I を集合とし, $(X_i)_{i\in I}$ を正規集合族とする. 選出関数

$$x : I \longrightarrow X, \quad x(i) \in X_i \ (\forall i \in I)$$

全体の集合を, $\prod_{i\in I} X_i$ と表す. 各 $j \in I$ に対し, 写像

$$pr_j : \prod_{i\in I} X_i \longrightarrow X_i, \quad x \longmapsto x(i)$$

を j 番目の **射影** という. 組

$$(\prod_{i\in I} X_i, (pr_i)_{i\in I}),$$

或いは, 単に, 集合 $\prod_{i\in I} X_i$ を集合族 $(X_i)_{i\in I}$ の **直積** といい, 各 X_i をその **直積因子** という.

補題 A.3.1 任意の $i \in I$ に対し, 射影 pr_i は全射である.

証明 任意の $x_i \in X_i$ をとる.

$$X'_j := X_j \ (j \neq i), \quad X'_i = \{x_i\}$$

とすると, $(X'_j)_{j\in I}$ は正規集合族である. 選出公理により, 選出関数

$$c : I \longrightarrow \bigcup_{i\in I} X_i \quad \text{s.t.} \quad c(i) \in X'_j$$

が存在する. このとき, $c \in \prod_{j\in I} X_j$ と見なせ, $pr_i(c) = c(i) = x_i$. よって, pr_i は全射である. □

定理 A.3.2 （直積の特徴付け）$(X_i)_{i\in I}$ を I を添数集合とする正規集合族とするとき，直積 $(\prod_{i\in I} X_i, (pr_i)_{i\in I})$ は，次の性質 (P) を満たす．

(P) 各 pr_i は全射で，任意の集合 Y と写像 $f_i : Y \longrightarrow X_i$ の組 $(Y, (f_i)_{i\in I})$ に対し，

$$\exists_1 f : Y \longrightarrow \prod_{i\in I} X_i \quad \text{s.t.} \quad pr_i \circ f = f_i \ (\forall i \in I).$$

また，組 $(D, (p_i)_{i\in I})$ も性質 (P) を満たせば，全単射

$$\phi : \prod_{i\in I} X_i \longrightarrow D \quad \text{s.t.} \quad pr_i = p_i \circ \phi \ (\forall i \in I)$$

が存在する．

証明 まず，直積 $(\prod_{i\in I} X_i, (pr_i)_{i\in I})$ が性質 (P) を満たすことを示す．前補題により，pr_i は全射である．写像 $f : Y \longrightarrow \prod_{i\in I} X_i$ を

$$f(y) = (f_i(y))_{i\in I}, \quad (y \in Y),$$

すなわち，

$$f(y) : I \longrightarrow X, \quad i \longmapsto f_i(y)$$

と定めると，$pr_i(f(y)) = f_i(y)$ が成り立つ．また，このような f は一意的に定まる．実際，$g : Y \longrightarrow \prod_{i\in I} X_i$ も $pr_i(f(y)) = f_i(y)$ $(\forall i \in I)$ を満たすとすれば，$f(y)(i) = g(y)(i)$ $(\forall i \in I)$．従って，$f(y) = g(y)$．ここで y も任意なので，$f = g$ を得る．

後半を示そう．$(D, (p_i)_{i\in I})$ が性質 (P) を持つので，写像

$$\phi : \prod_{i\in I} X_i \longrightarrow D \quad \text{s.t.} \quad p_i \circ \phi = pr_i \ (\forall i \in I)$$

が一意的に存在する．また，写像

$$\psi : D \longrightarrow \prod_{i\in I} X_i \quad \text{s.t.} \quad pr_i \circ \psi = p_i \ (\forall i \in I)$$

が一意的に存在する．このとき

$$\psi \circ \phi : \prod_{i\in I} X_i \longrightarrow \prod_{i\in I} X_i \quad pr_i \circ (\psi \circ \phi) = pr_i \ (\forall i \in I).$$

一方，恒等写像 $id_{\prod_{i\in I} X_i}$ も，$\psi \circ \phi$ と同じ性質を持つ．再び，性質 (P) により，$\psi \circ \phi = id_{\prod_{i\in I} X_i}$．同様にして，$\phi \circ \psi = id_D$．を得る．従って，補題 A.2.25 により，$\phi$ は全単射である． □

定理 A.3.3 正規集合族の直積は性質 (P) を持つ組として，同型を除き，一意的に定まる．

例 A.3.6 選出公理は次のように言い換えられる．正規集合族 $(X_i)_{i\in I}$ に対し

$$\prod_{i\in I} X_i \neq \emptyset.$$

例 A.3.7 X を集合 Y の部分集合とし, $\iota : X \longrightarrow Y$ を自然な単射とする. I を添数集合とする X の部分集合族 $(X_i)_{i\in I}$ と Y の部分集合族 $(Y_i)_{i\in I}$ に対し, $X_i \subseteq Y_i$ $(\forall i \in I)$ が成り立っているとする. 写像 $x : I \longrightarrow X$ と $\iota \circ x : I \longrightarrow Y$ とを同一視し,

$$\prod_{i\in I} X_i \subseteq \prod_{i\in I} Y_i$$

と見なす.

注意 A.3.2 集合族 $(X_i)_{i\in I}$ が正規集合族でない場合, すなわち, 或る i に対し, $X_i = \emptyset$ ならば, $\prod_{i\in I} X_i = \emptyset$ とする.

例 A.3.8 I を添数集合とする二つの集合族 $(X_i)_{i\in I}, (Y_i)_{i\in I}$ を考える. 各 $i \in I$ に対し, 写像 $f_i : X_i \longrightarrow Y_i$ が与えられたとする. 直積 $(\prod_{i\in I} Y_i, (q_i)_{i\in I})$ は, 定理 A.3.2 (P) を満たす. 従って, 組 $(\prod_{i\in I} X_i, (f_i \circ pr_i)_{i\in I})$ に対し, 写像

$$f : \prod_{i\in I} X_i \longrightarrow \prod_{i\in I} Y_i, \quad \text{s.t.} \quad q_i \circ f = f_i \circ pr_i \ (\forall i \in I)$$

が一意的に存在する. このとき

$$q_i(f((x_i)_{i\in I})) = f_i(x_i) \ (\forall i \in I), \text{ i.e. } f((x_i)_{i\in I}) = (f_i(x_i))_{i\in I}$$

が成り立つ.

f を

$$f = \prod_{i\in I} f_i$$

と表し, 写像の族 $(f_i)_{i\in I}$ の **直積** という.

例 A.3.9 集合族 $(X_i)_{i\in I}$ において, $X = X_i$ $(\forall i \in I)$ のとき, $\prod_{i\in I} X_i$ を

$$X^I$$

と表し, I 上の X の **配置集合** という. 定義より, X^I は, 集合 I から集合 X への写像全体のなす集合である：

$$X^I = \mathrm{Map}(I, X).$$

A.3.3 分割と直和

定義 A.3.4 X を空でない集合とする. X の部分集合のなす（I を添数集合とする）正規集合族 $(X_i)_{i\in I}$ は, 次を満たすとき, X の **分割** と呼ばれる:

(A.4) $\qquad X = \cup_{i\in I} X_i$

(A.5) $\qquad X_i \cap X_j = \emptyset \ (i \neq j \in I)$

このとき,

$$X = \sum_{i \in I} X_i$$

と表す.

(A.5) を満たす正規集合族は **分離的** であるという.

例 A.3.10 E を偶数全体の集合, O を奇数全体の集合とするとき, $\{E, O\}$ は, 整数全体のなす集合 $\mathbb{Z}$ の分割である.

例 A.3.11 $I = \{1, 2, \cdots, n\}$, 或いは, $I = \mathbb{N}$ とする. $(X_i)_{i \in I}$ が集合 X の分割とするとき

$$X = X_1 + \cdots + X_n, \quad X = X_1 + X_2 + \cdots$$

と表すこともある.

例 A.3.12 $f : X \longrightarrow Y$ を集合の写像とする. このとき, $\{f^{-1}(y) \mid y \in f(X)\}$ は X の分割である. この分割を P_f と表す.

定義 A.3.5 $(X_i)_{i \in I}$ を I を添数集合とする正規集合族とし, $X_i' := X_i \times \{i\}$ とする [2]. すると $i \neq j$ ならば $X_i' \cap X_j' = \emptyset$.

$$\coprod_{i \in I} X_i = \bigcup_{i \in I} X_i',$$

と表し

$$\iota_i : X_i \longrightarrow \coprod_{i \in I} X_i, \quad x \longmapsto (x, i)$$

と定める. このとき, 各 ι_i は単射で, $(\iota_i(X_i))_{i \in I}$ は $\coprod_{i \in I} X_i$ の分割である.

組 $(\coprod_{i \in I} X_i, (\iota_i)_{i \in I})$, 或いは単に, $\coprod_{i \in I} X_i$ を, 集合族 $(X_i)_{i \in I}$ の **直和** といい, X_i をその **直和因子** という.

定理 A.3.6 (直和の特徴づけ) $(X_i)_{i \in I}$ を正規集合族とするとき, 直和 $(\coprod_{i \in I} X_i, (\iota_i)_{i \in I})$ は, 次の性質 (S) を満たす.

(S) ι_i は単射で, $(\iota_i(X_i))_{i \in I}$ は $\coprod_{i \in I} X_i$ の分割である. さらに, 任意の集合 Y と任意の写像 $f_i : X_i \longrightarrow Y$ の組 $(Y, (f_i)_{i \in I})$ に対し,

$$\exists_1 f : X \longrightarrow Y \quad \text{s.t.} \quad f \circ \iota_i = f_i \ (\forall i \in I).$$

また, 組 $(C, (\lambda_i)_{i \in I})$ も性質 (S) を満たせば, 全単射

$$\phi : \coprod_{i \in I} X_i \longrightarrow C \quad \text{s.t. } \phi \circ \iota_i = \lambda_i \ (\forall i \in I)$$

が存在する.

[2] $(X_i)_{i \in I}$ が分離的ならば, この操作は不要である.

証明 直和 $(\coprod_{i\in I} X_i, (\iota_i)_{i\in I})$ が (S) を満たすことを示そう. ι_i は単射で, $(\iota_i(X_i))_{i\in I}$ は $\coprod_{i\in I} X_i$ の分割であることはよい. 更に, $x \in X_i$ に対し, $\phi((x,i)) = \lambda_i(x)$ と定めれば, $\phi \circ \iota_i = \lambda_i$ $(\forall i \in I)$ を満たし, このような f は一意的に定まる. 後半の証明は, 定理 A.3.2 の後半の証明と同様であるので省略する. □

定理 A.3.7 正規集合族の直和は性質 (S) を持つ組として, 同型を除き, 一意的に定まる.

注意 A.3.3 正規集合族 $(X_i)_{i\in I}$ が分離的の場合, すなわち, $X_i \cap X_j = \emptyset$ $(\forall i \neq j \in I)$ を満たすとき, 直和 $\coprod_{i\in I} X_i$ と和集合 $\cup_{i\in I} X_i$ は同じものである.

例 A.3.13 時に, X_i と $\iota_i(X_i)$ とを同一視する. また, $\coprod_{i\in I} X_i$ を $\sum_{i\in I} X_i$ とも書く. 更に, $I = \mathbb{N}$ のとき

$$\coprod_{i=1}^{\infty} X_i, \quad \sum_{i=1}^{\infty} X_i$$

と表し, $I = \{1, \cdots, n\}$ のとき

$$\coprod_{i=1}^{n} X_i, \quad \sum_{i=1}^{n} X_i, \quad X_1 + X_2 + \cdots + X_n$$

と表す.

注意 A.3.4 直積と直和は, 共通な仕方で定義されている. この共通性を **普遍性** という. また, 直積と直和の定義が互いに「逆」の関係になっている. この関係を **双対** という. 数学の概念はこのような普遍性を持つことが多い. また, 今後, 数学を学ぶ道々, 色々な双対に遭遇するであろう.

A.4 同値関係と商集合

A.4.1 二項関係

X, Y を集合とし, $(X, Y; R)$ を対応とする. 即ち, R を直積 $X \times Y$ の部分集合とする. このとき, 任意の $(x, y) \in X \times Y$ に対し,

$$x \sim_R y \quad ((x,y) \in R)$$
$$x \not\sim_R y \quad ((x,y) \notin R$$

と定める. $\sim_R$ を対応 $(X, Y; R)$ または R の定める X の元と Y の元との間の **関係** という.

特に, $X = Y$ のとき, $\sim_R$ を X **上の二項関係** という.

例 A.4.1 ２０２０年度N大学理工学部の学科の集合を $X = \{$ 数学科, 物理学科, $\cdots$, 土木工学科 $\}$ とし, 学生全体の集合を Y とする. 学生 y が 学科 x に属することを $y \prec x$ と表すことにし, $R = \{(x,y) \mid x \succ y\}$ とする. このとき, 学科 $x \in X$ に対し, x に属する学生の集合 $\{y \in Y \mid x \succ y\} = \{y \in Y \mid (x,y) \in R\}$ が定まる. 従って, X と Y の直積 $X \times Y$ の部分集合 R は, ”学生がどの学科に属するか” という ”関係” を定めている.

例 A.4.2 $f : X \longrightarrow Y$ を集合の写像とし, G_f をそのグラフとする. このとき, G_f の定める関係は次の通り：

$$x \sim_{G_f} y \quad \Longleftrightarrow \quad f = f(x).$$

例 A.4.3 $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ とするとき, R が定める二項関係は実数の大小関係 $\leq$ である.

例 A.4.4 X を集合とし,

$$R = \{(A, B) \in \mathcal{X} \times \mathcal{X} \mid A \subset B\}$$

とするとき, R が定める二項関係を, X の部分集合の **包含関係**という.

以後, 二項関係を考えるとき, 特に断らない限り, その二項関係を定める集合 R には言及しない.

A.4.2 同値関係

X を空でない集合とし, $\sim$ を X 上の二項関係とする. $\sim$ は次の三条件を満たすとき **同値関係**と呼ばれる：

（反射律）$x \sim x, \quad \forall x \in X,$

（対称律）$x \sim y \Longrightarrow y \sim x,$

（推移律）$x \sim y, y \sim z \Longrightarrow x \sim z.$

$x \sim y$ のとき, x は y に **同値** であるという.

例 A.4.5 X を空でない集合とする. 等号 $=$ は同値関係である. $=$ が定める部分集合 R は対角線集合

$$\triangle(X) = \{(x, x) \mid x \in X\}$$

である.

例 A.4.6 平面内の二つの三角形が合同であるという関係は同値関係である.

例 A.4.7 座標平面 $\mathbb{R}^2$ の 2 点 P, Q に対し, P を始点 Q を終点とする有向線分を $\overrightarrow{PQ}$ で表す. 二つの有向線分 $\overrightarrow{PQ}, \overrightarrow{RS}$ が, 向きが同じで, 長さが同じとき

$$\overrightarrow{PQ} \sim \overrightarrow{RS}$$

と定める. このとき $\sim$ は同値関係である. この同値関係の同値類を **平面ベクトル** という.

例 A.4.8 $m \in \mathbb{N}$ とする. $a, b \in \mathbb{Z}$ に対し

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad m | b - a$$

と定め, このとき, a は m を法として b に **合同** であるという. ここで, $m|b-a$ は m が $b-a$ を割り切る, すなわち, $b-a$ は m の倍数を意味する.

m の倍数全体の集合を (m) と表すと,

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad b - a \in (m).$$

(m) は次の性質を持つ.

(1) $0 \in (m)$,

(2) $a \in (m) \implies -a \in (m)$,

(3) $a, b \in (m) \implies a + b \in (m)$.

これらの性質により, $\equiv \pmod{m}$ が同値関係であることが判る.

例 A.4.9 $m \geq n$ とする. 複素数係数 (m, n) 行列全体の集合を $\mathrm{Mat}_{m\times n}(\mathbb{C})$ と表す. また, 複素数係数 l 次正則行列の全体を $\mathrm{GL}_l(\mathbb{C})$ と表す. $A, B \in \mathrm{Mat}_{m\times n}(\mathbb{C})$ に対し,

$$A \sim B \quad \Longleftrightarrow \quad A = PBQ \quad (\exists P \in \mathrm{GL}_m(\mathbb{C}), \exists Q \in \mathrm{GL}_n(\mathbb{C})$$

と定める.

$\mathrm{GL}_l(\mathbb{C})$ は, 次を満たす:

(1) $I_l \in \mathrm{GL}_l(\mathbb{C})$,

(2) $P \in \mathrm{GL}_l(\mathbb{C}) \implies P^{-1} \in \mathrm{GL}_l(\mathbb{C})$,

(3) $P, P' \in \mathrm{GL}_l(\mathbb{C}) \implies PP' \in \mathrm{GL}_l(\mathbb{C})$.

これらの性質により, $\sim$ が同値関係であることが判る.

$\sim$ を空でない集合 X に於ける同値関係とする. $x \in X$ と同値な元全体のなす X の部分集合を $C(x)$ または $[x]$ と表し, x を含む **同値類** という:

$$C(x) = \{y \in X | \, y \sim x\}$$

同値類 C は, 或る $x \in X$ に対し $C = C(x)$ と表されるが, このとき, x を同値類 C の **代表元** という. 同値類 C に含まれる任意の元が代表元となり得る.

同値関係 $\sim$ に関する同値類全体の集合を $X/\sim$ と表し, X の $\sim$ による **商集合** という. $X/\sim = \{C_i \mid i \in I\}$ とするとき, 各同値類 C_i から, 元 x_i を一つづつ選び出して得られる集合 $\{x_i \mid i \in I\}$ を $X/\sim$ の **完全代表系** という.

また, 写像

$$\pi : X \longrightarrow X/\sim, \quad x \longmapsto C(x)$$

は全射であり, **自然な全射** と呼ばれる.

例 A.4.10 ２０２０年度N大学理工学部１年生全体の集合を S とする. S に属するふたり a, b に対し, a, b が同じクラスに属するとき, $a \sim b$ と定義する. すると $\sim$ は同値関係であり, 同値類を, 数学科, 物理学科, 電子工学科などと呼んでいる：

$$S/\sim = \{\text{ 数学科, 物理学科, } \cdots\}.$$

数学科の学生 x, 物理学科の学生 y, $\cdots$ と各科から一人ずつ学生を選んで得られる集合 $\{x, y, \cdots\}$ は完全代表系である.

例 A.4.11 自然数 m を法とする整数の合同関係（例 A.4.8) において, $[i] = \{n \in \mathbb{Z} \mid m|n-i\}$ であり,

$$\mathbb{Z}/\equiv = \{[0], [1], \cdots, [m-1]\}.$$

この商集合を, 習慣で

$$\mathbb{Z}/(m)$$

と表す.

$[i]$ は m で割った余りが i となる整数全体の集合である. 従って, この場合, 同値類は m を法とする **剰余類** と呼ばれる. 明らかに,

$$\mathbb{Z} = [0] + [1] + \cdots + [m-1]$$

が成り立ち, 集合族 $([i])_{i \in I}$ $(I = \{0, 1, \cdots, m-1\})$ は, 整数の集合 $\mathbb{Z}$ の分割である.

$\{0, 1, \cdots, m-1\}$ は完全代表系である. また, $\{m, m+1, \cdots, 2m-1\}$ も完全代表系である.

定義から, 次を得る.

命題 A.4.1 $x, y \in X$ に対し, 次が成り立つ：

$$y \in C(x) \iff x \in C(y) \iff C(x) \cap C(y) \neq \emptyset$$

$$\iff x \sim y \iff C(x) = C(y).$$

問 A.4.2 上の命題を証明せよ.

命題 A.4.3 X を空でない集合とし, $\sim$ を X における同値関係とする. 適当な集合 I をとり, 同値類全体の集合を $\{C_i \mid i \in I\}$ とする. このとき, 集合族 $(C_i)_{i \in I}$ は, X の分割である：

$$X = \sum_{i \in I} C_i.$$

証明 右辺が左辺に含まれることは良い. C_i と C_j が異なる同値類ならば, 命題 A.4.1 により, $C_i \cap C_j = \emptyset$ が成り立つ. 逆に, X の任意の元 x に対し, x を含む同値類を C_i とすれば, $x \in C_i$ は, 右辺に含まれる. □

A.4.3 同値関係, 分割, 全射

1. 同値関係から分割.

X を空でない集合とし, $\sim$ を X 上の同値関係とし, $X/sim = \{C_i \mid i \in I\}$ とする. このとき, X の部分集合族 $P_\sim = (C_i)_{i \in I}$ は, 命題 A.4.3 により, 集合 X の分割であり, 同値関係 $\sim$ の定める分割と呼ばれる.

2. 分割から全射.

$P = (C_i)_{i\in I}$ を集合 X の分割とし, $Y := \{C_i \mid i \in I\}$ とする. このとき, 写像

$$\pi_P : X \longrightarrow Y, \quad x \longmapsto x \text{ を含む } C_i$$

は全射であり, 分割 P の定める全射と呼ばれる.

3. 全射から同値関係.

$f : X \longrightarrow Y$ を全射とする. このとき, $x, x' \in X$ に対し

$$x \sim_f x' \quad \Longleftrightarrow \quad f(x) = f(x')$$

とすると, $\sim_f$ は, X 上の同値関係であり, f の定める同値関係と呼ばれる.

補題 A.4.4 $f : X \longrightarrow Y$ と $f' : X \longrightarrow Y'$ を共に全射とする. このとき, f, f' の定める同値関係が一致する為必要十分条件は, 次の図が可換となる同型写像 $\phi : Y \longrightarrow Y'$ が存在することである:

$$\begin{array}{ccc} & f & \\ X & \longrightarrow & Y \\ f' \searrow & \circlearrowleft & \swarrow \phi \\ & Y' & \end{array}$$

但し, 図が可換であることを, 記号 $\circlearrowleft$ で表し, それは, $\phi \circ f = f'$ を意味する.

証明 十分性は明らかなので, 必要性のみを示す. 写像 $\phi : Y \longrightarrow Y'$ を次のように定める. $y \in Y$ に対し, $x \in f^{-1}(x)$ を取る.

$$x \in (f')^{-1}(f'(x)) \cap f^{-1}(y)$$

なので, 仮定により, $(f')^{-1}(f'(x)) = f^{-1}(y)$. 従って, $f'(x)$ は x のとり方に依らず定まる. そこで, $\phi(y) = f'(x)$ と定める. 容易にわかるように, ϕ が求めるもである. □

定理 A.4.5 (1) 同値関係が与えられたとき, 順に, 1,2,3 を施すと, 元の同値関係に戻る.

(2) 分割が与えられたとき, 順に, 2,3,1 を施すと, 元の分割に戻る.

(3) 全射 $f : X \longrightarrow Y$ が与えられたとき, 順に, 3,1,2 を施すと, 次の図が可換となる同型写像 $\phi : Y \longrightarrow Y' = \{f^{-1}(y) | \ y \in Y\}$ が存在する:

$$\begin{array}{ccc} & f & \\ X & \longrightarrow & Y \\ f' \searrow & \circlearrowleft & \swarrow \phi \\ & Y' & \end{array}$$

但し, 図が可換であることを, 記号 $\circlearrowleft$ で表し, それは, $\phi \circ f = f'$ を意味する. また f' は, 分割 $\{f^{-1}(y) | y \in Y\}$ の定める全射である.

証明 (1),(2) は, 明らかであろう. (3) は補題 A.4.4 より, 直ちに得られる. □

A.5 順序集合と Zorn の補題

A.5.1 順序集合

定義 A.5.1 M を集合とする. M 上の二項関係 $''\leq''$ は

(1) $x \leq x$,

(2) $x \leq y, y \leq z \Longrightarrow x \leq z$,

(3) $x \leq y, y \leq x \Longrightarrow x = y$,

を満たすとき **順序関係** と呼ばれる. 順序関係が定められた集合を **順序集合** という. 順序関係を明示する際は, 順序集合を組 $(M, \leq)$ で表す.

順序関係は, 更に

(4) 任意の $x, y \in M$ に対し $x \leq y$ または $y \leq x$

が成立つとき, **全順序関係** と呼ばれ, 全順序関係が定められた集合を **全順序集合** という.

例 A.5.1 $(M, \leq)$ を順序集合とする. $a, b \in M$ に対し, $a \leq b, a \neq b$ のとき, $a < b$ と表す. M は次のように分割される:

$$M = \{x \mid a < x\} + \{a\} + \{x \mid x < a\} + \{x \mid x \not\leq a, a \not\leq x\}.$$

例 A.5.2 X を集合とし, $\mathcal{P}(X)$ をその冪集合とする. $\mathcal{P}(X)$ における包含関係は順序関係であるが, 一般には, 全順序関係ではない.

例 A.5.3 $\mathbb{R}$ の大小関係 $\leq$ は全順序関係である.

例 A.5.4 自然数全体の集合 $\mathbb{N}$ において

$$m \leq n \quad \overset{def}{\Longleftrightarrow} \quad m|n$$

と定めると, $\leq$ は順序関係である.

例 A.5.5 空でない集合 X 上の実数値関数全体の集合を $\mathrm{Map}(X, \mathbb{R})$ と表す. $f, g \in \mathrm{Map}(X, \mathbb{R})$ に対し

$$f \leq g \quad \overset{def}{\Longleftrightarrow} \quad f(x) \leq g(x)\ (\forall x \in X)$$

と定めると, $\leq$ は順序関係である.

A.5.2 上界, 上限, 極大元, 下界, 下限, 極小元

定義 A.5.2 N を順序集合 M の部分集合とする. $x \in M$ は

$$y \leq x, \quad \forall y \in N$$

を満たすとき, N の **上界** と呼ばれる. N の上界のうち最小のものを N の **上限** といい,

$$\sup_M(N)$$

と表す. また $x \in N$ は, N の中に真に大きいものが存在しないとき, すなわち

$$y \in N,\ x \leq y \Longrightarrow x = y$$

を満たすとき N の **極大元** と呼ばれる. さらに, $a \in N$ が $x \leq a$ $(\forall x \in N)$ を満たすとき, a を N の **最大元** といい,

$$a = \max(N)$$

と表す.

同様に, 下界, 下限, 極小元, 最小元が定義される.

例 A.5.6 M を順序集合とし, N をその空でない部分集合とする. N の上限は存在すれば一意的に定まる.

例 A.5.7 例 A.5.3 の順序集合の部分集合 $E := \{(1+\frac{1}{n})^n \mid n \in \mathbb{N}\}$ に対し, 3 は一つの上界であり, 上限は自然対数の底 $e = 2.7182\cdots$ である.

問 A.5.3 例 A.5.4 の順序集合 $\mathbb{N}$ の部分集合 $\{4, 6\}$ の 上界, 上限, 下界, 下限を求めよ.

A.5.3 整列集合

定義 A.5.4 M を全順序集合とする. M の任意の空でない部分集合が最小元を持つとき, M を **整列集合** という.

例 A.5.8 整列集合の空でない部分集合は整列集合である.

例 A.5.9 自然数全体のなす全順序集合 $(\mathbb{N}, \leq)$ は整列集合である.

定理 A.5.5 （超限帰納法）$(M, \leq)$ を整列集合とする. M の元に関する或る命題 $P(x)$ $(x \in M)$ が, 次の性質を持つならば, $P(x)$ は M のすべての元に対し成り立つ.

(I) 任意の $x \in M$ に対し, $P(y)$ が $\{y \mid y < x\}$ の各元に対して成り立つならば, $P(x)$ が成り立つ.

証明 $P(x)$ が成り立たない x の集合を M' とする. もし $M' \neq \emptyset$ ならば, M は整列集合なので, M' には最小元 x_0 が存在する. すると集合 $\{y \mid y < x_0\}$ は M' と交わらない. 従って, $P(y)$ は $\{y \mid y < x_0\}$ の各元に対して成り立つ. すると (I) により, $P(x_0)$ も成り立ち, これは $x_0 \in M'$ に反する. これは不合理であり, よって M' は空でなければならない. よって $P(x)$ は任意の $x \in M$ に対して成り立つ. □

例 A.5.10 （数学的帰納法）$\mathbb{N}$ の元に関する或る命題 $P(x)$ $(x \in \mathbb{N})$ が, 次の性質を持つならば, $P(x)$ は $\mathbb{N}$ のすべての元に対し成り立つ.

(1) $P(1)$ が成り立つ,

(2) $P(n)$ が成り立つならば, $P(n+1)$ も成り立つ.

定義 A.5.6 M を整列集合とする. $m \in M$ に対し

$$M(m) := \{x \mid x \in M, x < m\}$$

を m の **下切片**, 或いは単に, **切片** という. m は, $M(m)$ の上界である.

例 A.5.11 整列集合 $(\mathbb{N}, \leq)$ において, $n \in \mathbb{N}$ の切片は $N(n) = \{1, 2, \cdots, n-1\}$.

定義 A.5.7 $(M, \leq), (M', \leq')$ を順序集合とし, $f : M \longrightarrow M'$ を写像とする.

$$x \leq y \quad \Longrightarrow f(x) \leq' f(y)$$

をみたすとき, f を **順序射** という. 更に, f が単射ならば, **順序単射**, f が全単射ならば, **順序同型射** という. M から M' への順序同型射が存在するとき, M と M' は **順序同型** であるといい, $M \simeq M'$ と表す.

補題 A.5.8 $(M, \leq)$ を整列集合とする. $f : M \longrightarrow M$ が順序単射ならば $x \leq f(x)$ $(\forall x \in M)$ が成り立つ.

証明 結論を否定しよう. すると, $f(x) < x$ となる x が存在する. 従って $M_0 := \{x \mid f(x) \leq x\}$ は空でない. M は整列集合なので, M_0 には最小元 x_0 が存在する. すると $f(x_0) < x_0$. f は順序単射なので, $f(f(x_0)) < f(x_0)$. 従って $f(x_0) \in M_0$ となる. $f(x_0) < x_0$ だったので, x_0 の最小性に反する. よって, 補題は成り立つ. □

補題 A.5.9 $(M, \leq)$ を整列集合, M' をその部分集合とする. $x \in M - M'$ が M' の上界ならば, M と M' は順序同型とはならない. 特に $m \in M$ に対し M と $M(m)$ は順序同型にならない. 更に, $m, n \in M$ $(m \neq n)$ に対し $M(m)$ と $M(n)$ とは順序同型にならない.

証明 順序同型射 $f : M \longrightarrow M'$ が存在したとする. $\iota : M' \longrightarrow M$ を標準的単射とすると, 合成射 $\iota \circ f : M \longrightarrow M$ は順序単射である. すると, 補題 A.5.8 により, $x \leq \iota(f(x))$. $\iota(f(x)) \in M'$ なので, x が M' の上界ということに反する. 従って, M と M' が順序同型ということは有り得ない. □

定理 A.5.10 （整列集合の比較定理）M, M' を整列集合とする. このとき次の内いずれか一つだけ必ず起こる:

(1) $M \simeq M'$,

(2) $M \simeq M'(m')$ $(\exists m' \in M')$,

(3) $M(m) \simeq M'$ $(\exists m \in M)$.

証明 M, M' の一方が空集合ならば, 明らかに成り立つ. そこで, M, M' は共に空集合でないとする. 補題 A.5.9 より, 次のことがわかる. (1) と (2) は両立しないし, (1) と (3) も両立しない. また, (2), (3) における m, m' は一意的に定まり, さらに (2) と (3) も両立しない.

$m_0 = \min M, m'_0 = \min M'$ とおき,

$$M_0 = \{x \in M \mid M(x) \simeq M'(x') \ (\exists x' \in M')\}$$

とする. $M(m_0) = \emptyset = M'(m'_0)$ なので, $m_0 \in M_0$ であり, $M_0 \neq \emptyset$. また,

$$x \in M_0 \quad \Longrightarrow \quad M(x) \subset M_0$$

が成り立つ. $M - M_0 \neq \emptyset$ ならば, $m_1 = \min\,(M - M_0)$ とすると, $M_0 = M(m_1)$ となる. さて, $x \in M_0$ に対し, $M(x) \simeq M'(x')$ となる x' は, 補題 hikaku0 より, 一意的に定まる. そこで, $x' = f(x)$ とおけば, 写像

$$f : M_0 \longrightarrow M'; \quad x \longmapsto x' = f(x)$$

は順序単射である. $M' - f(M_0) \neq \emptyset$ ならば, $m'_1 = \min\,(M' - f(M_0))$ とおけば, $f(M_0) = M'(m'_1)$. 従って, $M = M_0$ ならば, $M \simeq f(M) = M'$ または $M \simeq f(M) = M'(m'_1)$ が成り立つ. $M_0 \subsetneq M$ ならば, $M_0 = M(m_1)$. $f(M_0) = M'(m'_1)$ とすると, $M_0 = M(m_1) \simeq M'(m'_1)$ が成り立ち, M_0 の定義より, $m_1 \in M_0$. これは不合理であり, $f(M_0) = M'$ でなければならない. □

系 A.5.11 整列集合 M の部分集合は, M または M の切片に順序同型である. 任意の無限整列集合 M は, 自然数全体のなす整列集合 $\mathbb{N}$ に同型であるか, または, $\mathbb{N}$ と同型な切片を含む.

証明 M' を M の部分集合とする. 定理 A.5.10 により, 次のいずれかが成り立つ：

$$M \simeq M', \quad M \simeq M'(m') \ (\exists m' \in M'), \quad M(m) \simeq M' \ (\exists m \in M).$$

$f : M \longrightarrow M'(m')$ が順序同型射ならば, 標準的単射 $\iota : M'(m') \longrightarrow M$ との合成射 $g = f \circ \iota : M \longrightarrow M$ は順序単射. しかし $g(m') = f(m') \in M'(m')$ であり, $g(m') \leq m'$ となる. これは, 補題 A.5.8 に反する. 従って, $M' \simeq M$ であるか $M' \simeq M(m)$. もし $M \simeq \mathbb{N}(n)$ ならば, M は有限集合となり, 仮定に反する. 従って, 定理 A.5.10 より, 後半は得られる. □

補題 A.5.12 （整列集合の合併）M を集合とし, $(N_i)_{i \in I}$ をその部分集合族とする. 各 N_i 上に, 順序関係 $\leq_i$ が定義されていて, 次を満たすとする:

(1) $(N_i, \leq_i)$ は整列集合である,

(2) 相異なる i, j に対し, $(N_i, \leq_i)$ と $(N_j, \leq_j)$ のうち一方は他方の切片に一致する,

(3) 任意の二元 $x, y \in N := \cup_{i \in I} N_i$ に対し $x, y \in N_i$ となる i が存在する.

このとき, $x, y \in N$ に対し, $x, y \in N_i$ なる i をとり, $x \leq_i y, y \leq_i x$ に従って $x \leq y, y \leq x$ と定める. このとき $\leq$ は i の取り方によらず定まり, $(N, \leq)$ は整列集合となる.

証明 $\leq$ を定義する際, i の取り方によらないことは, 条件 (2) から得られる. また $(N, \leq)$ が全順序集合となることも, 条件 (1), (3) より容易にわかる. 最後に $(N, \leq)$ は整列集合であることを示す.

L を空でない N の部分集合とする. $N = \cup_{i \in I} N_i$ なので $L \cap N_i \neq \emptyset$ となる i が存在する. N_i は整列集合なので, $x_0 = \min(L \cap N_i)$ が存在する. $x \in L$ を任意にとる. $x \in N_i$ ならば $x_0 \leq x$. $x \notin N_i$ とすると, $x \in N_j$ となる j が存在する. このときは, 条件 (2) により, $(N_i, \leq_i)$ は $(N_j, \leq_j)$ の切片である. $x_0 \in N_i \subset N_j$ で $x \in N_j - N_i$ なので $x_0 < x$. 従って $\min(L) = x_0$ となり, N は整列集合である. □

A.5.4 Zorn の補題と Zermero の整列可能定理

定義 A.5.13 空でない順序集合 M は, 任意の全順序部分集合が（上限）上界をもつとき, **（強）帰納的順序集合** と呼ばれる.

補題 A.5.14 S を空でない強帰納的順序集合とし, 写像 $f : S \longrightarrow S$ は $s \leq f(s)$ $(\forall s \in S)$ を満たすとする. このとき, $f(s_0) = s_0$ を満たす $s_0 \in S$ が存在する.

証明 $S \neq \emptyset$ なので, $a \in S$ をとり, $S_1 = \{s \in S \mid a \not\leq s\}$ とし, $S' = S - S_1$ とすると, $a \in S'$ であり, $a \leq s$ $(\forall s \in S')$ が成り立つ.

S' の部分集合 R は, 次を満たすとき **認容** であるという：

(1) $a \in R$,

(2) $f(R) \subset R$,

(3) R の任意全順序部分集合 T に対し, T の上限は R に含まれる.

$s \in S'$ ならば, $a \leq s \leq f(s)$ なので, $f(s) \in S'$. 従って, S' は認容である. M を S' の全ての認容部分集合の共通部分とする. すると, M も認容であることが容易にわかる. M が全順序部分集合ならば, M の上限を b とするとき, (3) より, $b \in M$. よって, $b \leq f(b) \leq b$ となり, $f(b) = b$ を得る.

$c \in M$ は, 次を満たすとき **端点** であるという：

$$x \in M, x < c \quad \Longrightarrow \quad f(x) \leq c.$$

$x < a$ を満たす $x \in M$ は存在しないので, a は端点である.

補題 A.5.15 端点 c に対し,

$$M_c = \{x \in M \mid x \leq c \text{ または } f(c) \leq x\}$$

と定める. このとき, $M_c = M$ が成り立つ.

証明 $c \in M \subset S'$ なので $a \leq c$. よって, $a \in M_c$ が成り立つ. M_c が認容であれば, M の作り方より, $M = M_c$ を得る. さて, $f(M_c) \subset M_c$ を示そう. $x \in M_c$ を任意に取ると, M は認容なので, $f(x) \in M$. $x < c$ ならば, c は端点なので, $f(x) \leq c$. よって, M_c の定義より, $f(x) \in M_c$. $x = c$

ならば, $f(x) = f(c) \in M_c$. また, $f(c) \leq x$ ならば, $f(c) \leq x \leq f(x)$ となり, $f(x) \in M_c$. よって, $f(M_c) \subset M_c$ が示された.

T を M_c の全順序部分集合とし, T の上限を $b \in S$ とする. このとき, 定義より, $b \in S'$. M は認容なので, $b \in M$. c が T の上界ならば, $b \leq c$ となり, $b \in M_c$. また, $x \in T$ が $f(c) \leq x$ を満たすとすると, $f(c) \leq x \leq b$ となり, $b \in M_c$. □

補題 A.5.16 *$c \in M$ ならば, c は M の端点である.*

証明 E を M の端点の集合とする. すると, $a \in E$. E が認容であることを示す. まず, $c \in E$ ならば, $f(c) \in E$ が成り立つことを示そう. $x \in M = M_c$ とする. M_c の定義より, $x < c, x = c, f(c) \leq x$ のいずれかが成り立つ. よって, $x < f(c)$ ならば, $x < c$ か $x = c$ である. $x < c$ ならば, $f(x) \leq c \leq f(c)$. $x = c$ ならば, $f(x) = f(c)$. 従って, $f(c)$ が端点であることがわかり, $f(E) \subset E$.

T を E の全順序部分集合とし, T の上限を $b \in M$ とする. $b \in E$, 即ち, b は M の端点であることを示そう. そこで, $x \in M$ が $x < b$ を満たすとする. このとき, $f(c) \not\leq x$ となる $c \in T$ が存在する. さもなければ, $c \leq f(c) \leq x < b$ $(\forall c \in T)$ が成り立ち, x が T の上界となり, b の取り方に反する. $b \in M_c = M$ なので, $b \leq c$ または $f(c) \leq b$ が成り立つ. $b \leq c$ のとき, b は T の上限なので, $b \leq c \leq b$. よって, $b = c \in T \subset E$. 次に, $f(c) \leq b$ とする. さて, $x \in M_c = M$ なので, c の取り方より, $x \leq c$. $x < c$ ならば, c は端点なので $f(x) \leq c \leq b$. $x = c$ ならば, $f(x) = f(c) \leq b$. 従って, $b \in E$. よって, E は認容である. M の最小性より, $M = E$ を得る. □

M は全順序集合である. 実際, $x, y \in M$ とすると, $y \in M = M_x$. 従って, $y \leq x$ であるか $x \leq f(x) \leq y$ が成り立つ. よって, 上で示した様に, 補題 A.5.14 の証明が終わる. □

M の上限を s_0 とすると, $s_0 \leq f(s_0) \in M$. よって, $s_0 \leq f(s_0) \leq s_0$ となり, $s_0 = f(s_0)$. □

定理 A.5.17 *（Zorn の補題 I）空でない強帰納的順序集合は極大元を持つ.*

定理 A.5.18 *（Zorn の補題 II）空でない帰納的順序集合は極大元を持つ.*

定理 A.5.19 *（Zelmero の整列可能定理）任意の集合は, 適当な順序関係を定義すれば, 整列集合にすることが出来る.*

定理 A.5.20 次は同値である：

(1) 選出公理.

(2) Zorn の補題 *I*.

(3) Zorn の補題 *II*.

(4) *Zermero* の整列可能定理

証明 (1) $\Longrightarrow$ (2) M を強帰納的順序集合とする. M には極大元がないとすると, 各 $x \in M$ に対し,

$$M_x = \{y \in M \mid y > x\} \neq \emptyset.$$

すると, 選出公理により, 写像 $f : M \longrightarrow M$ で $\phi(x) > x$ $(\forall x \in M)$ となるものが存在する. しかし, M は強帰納的なので, 補題 A.5.14 により, $f(x_0) = x_0$ となる, $x_0 \in M$ が存在するが, これは不合理である. 従って, M には極大元が存在する.
(2) $\Longleftrightarrow$ (3) M を帰納的順序集合とする. M の空でない全順序部分集合全体を $\mathcal{T}$ とする. $x \in M$ とすれば, $\{x\} \in \mathcal{T}$ なので, $\mathcal{T} \neq \emptyset$. 順序集合 $(\mathcal{T}, \subset)$ を考える. $L := (N_i)_{i \in I}$ をその全順序部分集合とする. このとき $N = \cup_{i \in I} N_i$ は, L の上限である. 従って, $\mathcal{T}$ は強帰納的順序集合である. よって, $\mathcal{T}$ は極大元 N を持つ. M は帰納的順序集合なので, N は上界 x を持つ. $x \leq y$ とするとき, $N \cup \{y\}$ は, M の全順序部分集合なので, N の極大性より, $N = N \cup \{y\}$. よって, $y \leq x$ となり, x は M の極大元である. 逆は自明である.

(2) $\Longrightarrow$ (4) M を順序集合とする. $M = \emptyset$ ならば, 明らかであるので, $M \neq \emptyset$ とする.

$$\mathcal{N} := \{(N, \leq) \mid N \subset M,\ (N, \leq) \text{は整列集合}\ \}$$

とおく. $x \in M$ のとき, $\{x\}$ には, 一意的に順序関係 $\leq$ が定義され, $(\{x\}, \leq)$ は整列集合. 従って $\mathcal{N} \neq \emptyset$. $\mathcal{N}$ に次のようにして順序 $\preceq$ を定める: $(N, \leq), (N', \leq') \in \mathcal{N}$ に対し, $(N, \leq)$ が $(N', \leq')$ の切片となっているとき, $(N, \leq) \preceq (N', \leq')$ と定める. このとき, $(\mathcal{N}, \preceq)$ は帰納的順序集合となる. 実際, $\mathcal{N}_0$ を $\mathcal{N}$ の全順序部分集合とする.

$$N_0 = \cup_{N \in \mathcal{N}_0} N$$

とすると, 補題 A.5.12 により, N_0 には, 順序関係 $\leq_0$ が定められ,

$$(N, \leq) \preceq (N_0, \leq_0), \quad \forall (N, \leq) \in \mathcal{N}_0$$

であり, $(N_0, \leq_0)$ は整列集合となる. 従って, $(N_0, \leq_0) \in \mathcal{N}$ であり, $(N_0, \leq_0)$ は $\mathcal{N}_0$ の上限である. よって, $(\mathcal{N}, \preceq)$ は強帰納的順序集合である. 従って, 仮定により, $\mathcal{N}$ には極大元 $(N_1, \leq_1)$ が存在する. もし, $N_1 \subsetneq M$ ならば, $x \in M - N_1$ が存在する. $N_2 := N_1 \cup \{x\}$ とし, 順序 $\leq_2$ を, 次のように定める. N_1 の元については, もともとの順序 $\leq_1$ とし, N_1 の任意の元 x_1 に対し, $x_1 \leq_2 x$ とする. そうすると, $(N_2, \leq_2)$ は整列集合であり, $(N_2, \leq_2) \in \mathcal{N}$. 作り方より, $(N_1, \leq_1)$ は $(N_2, \leq_2)$ の切片なので, $(N_1, \leq_1)$ の極大性に反する. よって, $M = N_1$ となり, 証明を終わる.

(4) $\Longrightarrow$ (1) $(M_i)_{i \in I}$ を任意の正規集合族とする. $M := \cup_{i \in I} M_i$ に適当な順序関係 $\leq$ を定義し, $(M, \leq)$ を整列集合とする. $c(i) = \min(M_i)$ とすると

$$c : I \longrightarrow M, \quad c(i) \in M_i$$

は選出関数となる. □

Zorn 補題の応用として, 線形空間の基底の存在定理を示そう.

k を体とする. 体の概念に不慣れの際は, k は複素数体, 或いは実数体と限定してよい. V を k 上の線形空間とする. V の部分集合 B は, 次を満たすとき, V の基底と呼ばれる.

(1) B に含まれる空でない有限部分集合は k 上一次独立である. このとき, B は一次独立であるという.

(2) V の任意の元は, B に含まれる元の k 係数一次結合として表される.

定理 A.5.21 $V \neq \{0\}$ を k 上の線形空間とするとき, V には基底が存在する.

証明 一次独立な V の部分集合の全体を $\mathcal{B}$ とおく. $V \neq \{0\}$ なので, 零ベクトルと異なる $x \in V$ が存在する. このとき, $\{x\}$ は一次独立なので, $\mathcal{B} \neq \emptyset$. $\mathcal{B}$ は包含関係により, 順序集合となる. $(\mathcal{B}, \subset)$ は帰納的順序集合となることを示す. $\{B_i\}_{i\in I}$ を $\mathcal{B}$ の全順序部分集合とする.

$$B = \cup_{i\in I} B_i$$

とする. B の有限部分集合 F は, $\{B_i\}_{i\in I}$ が全順序部分集合なので, ある B_i に含まれる. 従って, F は k 上一次独立である. よって, B は一次独立であり, $B \in \mathcal{B}$. また, 定義より, B は $\{B_i\}_{i\in I}$ の上限である. 従って, $\mathcal{B}$ は帰納的順序集合である.

Zorn の補題により, $\mathcal{B}$ には極大元 B_0 が存在する. $B_0 \in \mathcal{B}$ なので, B_0 は一次独立である. $y \in V$ を任意に取る. $y \in B_0$ ならば, y は B_0 の一次結合で表される. $y \notin B_0$ とする. B_0 は極大元なので, $B_0 \cup \{y\}$ は一次独立でない. 従って, 一次従属な有限集合

$$\{x_1, x_2, \cdots, x_n\}$$

が存在し,

$$c_1x_1 + \cdots + c_nx_n = 0 \quad (c_1, \cdots, c_n \in k).$$

このとき, $c_1 \neq 0, \cdots, c_n \neq 0$ としてよい. また, B_0 は一次独立なので, $y = x_1$ としてよい. すると,

$$y = x_1 = -1/c_1(c_2x_2 + \cdots + c_nx_n)$$

となり, y は B_0 の一次結合である. よって, B_0 は基底である. □

A.6 濃度

A.6.1 濃度とその大小

この小節では, 集合の「大きさ」を論ずる. n 個の元からなる集合から, 自然数 n の概念が抽出された. その一般化として **濃度**（cardinality）の概念を得る.

全ての集合の集まりを考え, それを **宇宙** といい, $\mathcal{U}$ と表す. 注意 **??** に於いて確かめた様に, 宇宙 $\mathcal{U}$ は集合でない. さて, 集合 X に対し, X と対等, 即ち, 同型な集合の全体を $\mathrm{card}(X)$ と表し, X の **濃度** という.

n 個の元からなる有限集合 X の濃度を n と定める：

$$\mathrm{card}(X) = n.$$

定義より, 集合 X と Y が対等である為の必要十分条件は, それらの濃度が等しいことである：

$$X \simeq Y \iff \mathrm{card}(X) = \mathrm{card}(Y).$$

問 A.6.1 X, Y, Z を集合とするとき, 次が成り立つことを確かめよ：

(1) $\mathrm{card}(X) = \mathrm{card}(X)$.

(2) $\mathrm{card}(X) = \mathrm{card}(Y)$ ならば $\mathrm{card}(Y) = \mathrm{card}(X)$.

(3) $\mathrm{card}(X) = \mathrm{card}(Y)$, $\mathrm{card}(Y) = \mathrm{card}(Z)$ ならば $\mathrm{card}(X) = \mathrm{card}(Z)$.

集合 X から集合 Y への単射が存在するとき, X の濃度 $\mathrm{card}(X)$ は Y の濃度 $\mathrm{card}(Y)$ 以下であるといい,

$$\mathrm{card}(X) \leq \mathrm{card}(Y)$$

と表す. また, $\mathrm{card}(X) \leq \mathrm{card}(Y)$ であり, 等号が成り立たないとき,

$$\mathrm{card}(X) < \mathrm{card}(Y)$$

と表す.

問 A.6.2 濃度の大小は, 集合 X, Y の取り方に依らないことを確かめよ.

問 A.6.3 X, Y, Z を集合とするとき, 次が成り立つことを確かめよ：

(1) $\mathrm{card}(X) \leq \mathrm{card}(X)$.

(2) $\mathrm{card}(X) \leq \mathrm{card}(Y), \mathrm{card}(Y) \leq \mathrm{card}(Z) \implies \mathrm{card}(X) \leq \mathrm{card}(Z)$.

(3) $\mathrm{card}(X) \leq \mathrm{card}(Y), \mathrm{card}(Y) \leq \mathrm{card}(X) \implies \mathrm{card}(X) = \mathrm{card}(Y)$.

定理より, 直ちに次を得る：

系 A.6.4 X, Y, Z を集合とするとき,

$$\mathrm{card}(X) \leq \mathrm{card}(Y) \leq \mathrm{card}(Z), \mathrm{card}(X) = \mathrm{card}(Z) \quad \Longrightarrow \quad \mathrm{card}(X) = \mathrm{card}(Y) = \mathrm{card}(Z).$$

二つの集合の濃度は, 常に比較されることを示す次の定理の証明には, 整列可能定理 A.5.19 が用いられる.

定理 A.6.5 X, Y を集合とする. このとき, $\mathrm{card}(X) \leq \mathrm{card}(Y)$, または, $\mathrm{card}(X) \geq \mathrm{card}(Y)$ が成り立つ.

証明 整列可能定理（定理 A.5.19）により, 適当に順序を定義することにより, X, Y は整列集合にすることが出来る. すると, 整列集合の比較定理（定理 A.5.10）により, 次のいずれかの順序同型が成り立つ:

(1) $X \simeq Y$.

(2) $X \simeq Y(y)$ $(\exists y \in Y)$.

(3) $X(x) \simeq Y$ $(\exists x \in X)$.

特に, X から Y, または, Y から X への単射が存在する. 従って, $\mathrm{card}(X) \leq \mathrm{card}(Y)$, または, $\mathrm{card}(X) \geq \mathrm{card}(Y)$ が成り立つ. □

例題 A.6.6 $\mathrm{card}(X) \leq \mathrm{card}(Y)$ ならば, $\mathrm{card}(X + X') = \mathrm{card}(Y)$ を満たす集合 X' が存在することを示せ.

（解） 仮定より, 単射 $f : X \longrightarrow Y$ が存在する. $X' = Y - f(X)$ とする. このとき, X と X' の直和 $X + X'$ と Y は同型となり, $\mathrm{card}(X + X') = \mathrm{card}(Y)$. □

A.6.2 可算集合と非可算集合

自然数全体の集合 $\mathbb{N}$ と同型な集合を **可算集合** という. 可算集合の濃度を $\aleph_0$ と表す：

$$\mathrm{card}(\mathbb{N}) = \aleph_0.$$

一方,

$$\mathrm{card}(X) > \aleph_0$$

を満たす集合 X を **非可算集合** という.

命題 A.6.7 X を無限集合とするとき, $\mathrm{card}(X) \geq \aleph_0$.

証明 X に適当な順序を定め, X を整列集合とする. すると, 整列集合の比較定理（定理 A.5.10）により, 次の順序同型のいずれかが成り立つ：

$$\mathbb{N} \simeq X, \quad \mathbb{N} \simeq X(x)\ (\exists x \in X), \quad \mathbb{N}(n) \simeq X\ (\exists n \in \mathbb{N}).$$

しかし, 最後の場合, X は有限集合となり, 不合理である. □

例 A.6.1 E_0 を正の偶数全体の集合とすれば, $\mathrm{card}(E_0) = \aleph_0$.

例題 A.6.8 $\mathrm{card}(\mathbb{Z}) = \aleph_0$.

（解） 写像

$$\mathbb{N} \longrightarrow \mathbb{Z}, \quad 1 \longmapsto 0,\ 2n \longmapsto n,\ 2n+1 \longmapsto -n$$

は全単射である. □

例題 A.6.9 $\mathrm{card}(\mathbb{Z} \times \mathbb{N}) = \mathrm{card}(\mathbb{N} \times \mathbb{N}) = \aleph_0$.

（解） $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ を

$$(i, j) \longmapsto 2^{i-1}(2j - 1)$$

と定めると, f は全単射となり, $\mathrm{card}(\mathbb{N} \times \mathbb{N}) = \aleph_0$. □

例題 A.6.10 $\mathbb{Q}$ は可算集合である.

（解） 有理数は既約分数 m/n, $(m \in \mathbb{Z}, n \in \mathbb{N})$ として一意的に表される. 従って, $\mathbb{Q}$ は既約分数 m/n 全体の集合と見なせる.

$$f : \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{N}, \quad m/n \longmapsto (m, n)$$

単射である. よって, $\aleph_0 = \mathrm{card}(\mathbb{N}) \leq \mathrm{card}(\mathbb{Q}) \leq \mathrm{card}(\mathbb{Z}\times\mathbb{N})$. 例題 A.6.9 により, $\mathrm{card}(\mathbb{Z}\times\mathbb{N}) = \aleph_0$. 更に, 定理 **??** の系により, $\mathrm{card}(\mathbb{Q}) = \aleph_0$ となり, $\mathbb{Q}$ は可算集合である. □

実数全体の集合 $\mathbb{R}$ の濃度を $\mathfrak{c}$ と表し, **連続体濃度** という.

問 A.6.11

$$\mathrm{card}((0,1)) = \mathrm{card}(\mathbb{R}).$$

定理 A.6.12

$$\aleph_0 < \mathfrak{c}.$$

証明 (Cantor の対角線論法) 任意の写像

$$f : \mathbb{N} \longrightarrow \mathbb{R}$$

をとる. $f(n)$ を十進小数で表す:

$$f(n) = a^{(n)}_{-i_n} a^{(n)}_{-i_n+1} \cdots a^{(n)}_{-1} . a^{(n)}_1 a^{(n)}_2 \cdots a^{(n)}_n \cdots .$$

ここで

$$a^{(n)}_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

$m = 1, 2, \cdots$ に対し

$$b_m = \begin{cases} 1 & (a^{(m)}_m \neq 1) \\ 0 & (a^{(m)}_m = 1) \end{cases}$$

と定める. すると任意の $n \in \mathbb{N}$ に対し, $f(n)$ と b との, 小数第 n 桁は, それぞれ,

$$a^{(n)}_n, \quad b_n.$$

b の選び方より, これらは異なり, $f(n) \neq b$. 従って f は全射では有り得ない. よって, 全単射 $f : \mathbb{N} \longrightarrow \mathbb{R}$ は存在し得ない. 従って, $\mathbb{N} \not\simeq \mathbb{R}$. 一方, $\mathbb{N} \subset \mathbb{R}$ なので, $\aleph_0 < \mathfrak{c}$. □

定理は

「実数全体のなす無限は, 自然数全体のなす無限より真に大きい.」

という驚くべきことを主張している.

注意 A.6.1 次の命題を **連続体仮説** といい, 未解決の問題である.
$\aleph_1$ を $\aleph_0$ の次に大きい濃度とする. このとき, $\aleph_1 = \mathfrak{c}$. 即ち,

$$\aleph_0 \leq \mathfrak{m} \leq \mathfrak{c} \quad \Longrightarrow \quad \aleph_0 = \mathfrak{m} \text{ または } \mathfrak{m} = \mathfrak{c}.$$

A.6.3 濃度の演算

X, Y を集合とし,

$$\mathfrak{m} = \mathrm{card}(X), \quad \mathfrak{n} = \mathrm{card}(Y)$$

と表す. X, Y の直和 $X + Y$, 直積 $X \times Y$ に対し,

$$\mathrm{card}(X + Y) = \mathfrak{m} + \mathfrak{n}, \quad \mathrm{card}(X \times Y) = \mathfrak{m}\mathfrak{n}$$

と定める. また, X 上の Y の配置集合 $X^Y = \mathrm{Map}(Y, X)$ に対し,

$$\mathrm{card}(X^Y) = \mathfrak{m}^{\mathfrak{n}}$$

と定める.

例題 A.6.13 $\mathfrak{m}, \mathfrak{n}, \mathfrak{p}$ を濃度とするとき, 次が成り立つことを証明せよ.

(1) $(\mathfrak{m}^{\mathfrak{n}})^{\mathfrak{p}} = \mathfrak{m}^{\mathfrak{n}\mathfrak{p}}$.

(2) $\mathfrak{m} \geq \mathfrak{n}$ ならば, $\mathfrak{m}^{\mathfrak{p}} \geq \mathfrak{n}^{\mathfrak{p}}$.

(3) $\mathfrak{m} \geq \mathfrak{n}$ となる為の必要十分条件は $\mathfrak{m} = \mathfrak{n} + \mathfrak{p}$ となる濃度 $\mathfrak{p}$ が存在することである.

(解) $\mathfrak{m} = \mathrm{card}(M), \mathfrak{n} = \mathrm{card}(N), \mathfrak{p} = \mathrm{card}(P)$ とする.
(1) 例 A.2.21 より,

$$\mathrm{Map}(P, \mathrm{Map}(N, M)) \simeq \mathrm{Map}(P \times N, M).$$

両辺の濃度を取り, 結論を得る.
(2) 仮定により, 単射 $f : N \longrightarrow M$ が存在する. このとき,

$$\mathrm{Map}(P, N) \longrightarrow \mathrm{Map}(P, M); \quad \phi \longmapsto f \circ \phi$$

は単射である. よって, 両辺の濃度を取り, 結論を得る.
(3) 単射 $f : N \longrightarrow M$ が存在するならば, $P = M - f(N)$ とすると, $\mathfrak{m} = \mathrm{card}(f(N)) + \mathfrak{P} = \mathfrak{n} + \mathfrak{p}$.
逆は明らか. □

命題 A.6.14 $\mathfrak{m} \leq \aleph_0$ ならば, $\mathfrak{m} + \aleph_0 = \mathfrak{m}$.

証明 $\mathfrak{m} = \mathrm{card}(M) < \aleph_0$ ならば, M は有限集合である. $M = \{x_1, \cdots, x_n\}$ とし,

$$f : \mathbb{N} \longrightarrow X + \mathbb{N}$$

を

$$i \longmapsto x_i \ (1 \leq i \leq n), \quad j \longmapsto j - n \ (j > n)$$

とすると, f は全単射である. $\mathfrak{m} = \mathrm{card}(M) = \aleph_0$ のとき, $M = \mathbb{N}' = \{1', 2', \cdots, n', \cdots\}$ と仮定して良い. $f : \mathbb{N}' + \mathbb{N} \longrightarrow \mathbb{N}$ を

$$n' \longmapsto 2n - 1, \quad n \longmapsto 2n$$

と定めると, f は全単射となり, $\mathfrak{m} + \aleph_0 = \aleph_0$. □

命題 A.6.15 $0 < \mathfrak{m} \leq \aleph_0$ を満たすならば, $\mathfrak{m}\aleph_0 = \aleph_0$.

証明 $\mathfrak{m} = \mathrm{card}(M)$ とし, M が空でない有限集合の場合. $\mathrm{card}(M) = n$ とする. $n = 1$ のとき明らかで, $n = 2$ の場合は, 命題 A.6.14 に於いて, $\mathrm{card}(M) = \aleph_0$ の場合である. 一般の n の場合は帰納法により直ちに得られる. $\mathrm{card}(M) = \aleph_0$ の場合 $M = \mathbb{N}$ として良く, 例題 A.6.9 より, $\mathfrak{m}\aleph_0 = \aleph_0$. □

定理 A.6.16 $\mathfrak{m} \geq \aleph_0$ ならば, $\mathfrak{m} = \aleph_0\mathfrak{p}$ を満たす濃度 $\mathfrak{p}$ が存在する.

証明 $\mathfrak{m} = \mathrm{card}(X)$ の部分可算集合全体の集合を

$$\mathcal{C} = \{N \in \mathcal{P}() \mid \mathrm{card}(N) = \aleph_0\}$$

とする. $\mathcal{C}$ の空でない部分集合 $\mathcal{N}$ で集合族 $(N)_{N\in\mathcal{N}}$ は分離的, すなわち, $N \cap N' = \emptyset$ $(\forall N \neq N' \in \mathcal{N})$, なものを考える. このような $\mathcal{N}$ の全体を S と表す. S は, 包含関係を順序として, 強帰納的順序集合となる. 従って, Zorn の補題 I（定理 **??**）により, S には極大元 $\mathcal{N}_0$ が存在する.

$$X_0 = \sum_{N\in\mathcal{N}_0} N, \quad X_1 = X - X_0$$

とおく. このとき, $\mathrm{card}(X_1) < \aleph_0$. 実際, $\mathrm{card}(X_1) \geq \aleph_0$ とすると, X_1 は濃度 $\aleph_0$ の部分集合 N_1 を含む. $\mathcal{N}_1 = \mathcal{N} \cup \{N_1\}$ も S に含まれ, $\mathcal{N}_0$ の極大性に反する. さて, $N_0 \in \mathcal{N}_0$ を任意にとると, 命題 A.6.15 により, $N_0 + X_1 \simeq N_0$. $\mathcal{N}_0$ の N_0 を $N_0 + X_1$ に置き換え, 他の元はそのままとして得られる集合を $\mathcal{N}_0'$ とすると, $X = \sum_{N\in\mathcal{N}_0'} N$. 各 $N \in \mathcal{N}_0'$ に対し, 全単射

$$f_N : \mathbb{N} \longrightarrow N$$

が存在する. このとき,

$$f : \mathbb{N} \times \mathcal{N}_0' \longrightarrow X = \sum_{N\in\mathcal{N}_0'} N; \quad (n, N) \longmapsto f_N(n)$$

は全単射である. □

定理 A.6.17 $\mathfrak{m} \geq \aleph_0$, $\mathfrak{m} \geq \mathfrak{n}$ ならば, $\mathfrak{m} + \mathfrak{n} = \mathfrak{m}$.

証明 $\mathfrak{m} = \mathrm{card}(X), \mathfrak{n} = \mathrm{card}(Y)$ とする. Y が有限集合の場合. $\mathfrak{m} \geq \aleph_0$ なので, $\mathfrak{m} = \aleph_0 + \mathfrak{p}$ を満たす濃度 $\mathfrak{p}$ が存在する. 従って,

$$\mathfrak{m} + \mathfrak{n} = (\mathfrak{p} + \aleph_0) + \mathfrak{n} = \mathfrak{p} + (\aleph_0 + \mathfrak{n}).$$

命題 A.6.14 より, $\aleph_0 + \mathfrak{n} \simeq \aleph_0$ であり, $\mathfrak{m} + \mathfrak{n} = \mathfrak{p} + \aleph_0 = \mathfrak{m}$ を得る.

$\mathfrak{n} \geq \aleph_0$ の場合. 定理 A.6.16 により, $\mathfrak{n} = \aleph_0\mathfrak{p}$ を満たす濃度 $\mathfrak{p}$ が存在する. $\mathfrak{m} \geq \mathfrak{n}$ なので, $\mathfrak{m} = \mathfrak{m}+\mathfrak{q}$ を満たす濃度 $\mathfrak{q}$ が存在し,

$$\mathfrak{m} = \mathfrak{n} + \mathfrak{q} = \aleph_0\mathfrak{p} + \mathfrak{q}.$$

従って,

$$\begin{aligned}\mathfrak{m}+\mathfrak{n} &= (\mathfrak{q}+\aleph_0\mathfrak{p})+\aleph_0\mathfrak{p}\\ &= \mathfrak{q}+(\aleph_0\mathfrak{p}+\aleph_0\mathfrak{p})\\ &= \mathfrak{q}+(\aleph_0+\aleph_0)\mathfrak{p}\\ &= \mathfrak{q}+\aleph_0\mathfrak{p}\end{aligned}$$

となり, $\mathfrak{m}+\mathfrak{n}=\mathfrak{m}$. □

系 A.6.18 （Bernstein の定理）$\mathfrak{m}\geq\mathfrak{n}$, $\mathfrak{m}\leq\mathfrak{n}$ ならば $\mathfrak{m}=\mathfrak{n}$.

証明 これは, 定理 **??** であるが, その別証である. $\mathfrak{m}$ が有限のときは明らか. よって, $\mathfrak{m}\geq\aleph_0$ としてよい. このとき, $\mathfrak{n}\geq\aleph_0$ であり, 定理より, $\mathfrak{m}=\mathfrak{m}+\mathfrak{n}=\mathfrak{n}$. □

例題 A.6.19 有理整数係数の代数方程式

$$f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_0=0\quad(a_n\neq0)$$

の解である複素数を **代数的数** という. 代数的数全体のなす集合は可算集合であることを示せ.

証明 代数方程式 $f(X)$ に対し, その高さ $h(f)$ を

$$h(f)=n+|a_n|+|a_{n-1}|+\cdots+|a_0|$$

により定義する. 各自然数 N に対し, 高さが N である代数方程式は有限個であり, 更に, これら代数方程式の解である複素数も有限個である. 即ち, 高さ N の代数方程式の解の集合を S_N とすると, $|S_N|<\infty$. 代数的数の集合を $\bar{\mathbb{Q}}$ とするとき,

$$\bar{\mathbb{Q}}=\cup_{N\in\mathbb{N}}S_N.$$

従って,

$$\mathrm{card}(\bar{\mathbb{Q}})\leq\mathrm{card}(\mathbb{N}\times\mathbb{N})=\mathrm{card}(\mathbb{N})=\aleph_0$$

となり, $\bar{\mathbb{Q}}$ は可算集合である. □

定理 A.6.20 $\mathfrak{m}\geq\aleph_0$, $\mathfrak{m}\geq\mathfrak{n}>0$ ならば, $\mathfrak{mn}=\mathfrak{m}$.

証明 $\mathfrak{m}=\mathfrak{n}$ の場合. $\mathfrak{m}=\mathrm{card}(X)$ とする. 集合

$$S=\{(N,f)\mid N\subset X, f:N\times N\longrightarrow N\text{ は全単射 }\}$$

を考える. $\mathrm{card}(X)\geq\aleph_0$ なので, $S\neq\emptyset$.

$$(N,f)\leq(N',f')\quad\Longleftrightarrow\quad N\subset N',\ f'|_{N\times N}=f$$

とすると, $(S,\leq)$ は強帰納的順序集合である. 従って, Zorn の補題　I（定理 **??**）により, 極大元 (N_0,f_0) が存在する.

$N_1 = X - N_0$ とする. $\mathrm{card}(N_0) \geq \mathrm{card}(N_1)$ とすると, $X = N_0 + N_1, \mathrm{card}(N_0) \geq \aleph_0$. よって, 定理 A.6.17 により

$$\mathrm{card}(X) = \mathrm{card}(N_0) + \mathrm{card}(N_1) = \mathrm{card}(N_0) = \mathrm{card}(N_0 \times N_0) = \mathrm{card}(X \times X).$$

次に, $\mathrm{card}(N_0) < \mathrm{card}(N_1)$ は起こりえないことを示す. もし, そうならば, N_1 は N_0 と同型な部分集合 N_0' を含む. 直和 $N_0 + N_0'$ を考えると

$$(N_0 + N_0') \times (N_0 + N_0') = N_0 \times N_0 + N_0 \times N_0' + N_0' \times N_0 + N_0' \times N_0'.$$

$$P := N_0 \times N_0' + N_0' \times N_0 + N_0' \times N_0'$$

とすると, 定理 A.6.17 を用いて,

$$\begin{aligned} \mathrm{card}(P) &= \mathrm{card}(N_0 \times N_0') + \mathrm{card}(N_0' \times N_0) + \mathrm{card}(N_0' \times N_0') \\ &= \mathrm{card}(N_0 \times N_0 + N_0 \times N_0 + N_0 \times N_0) \\ &= \mathrm{card}(N_0 \times N_0) = \mathrm{card}(N_0) = \mathrm{card}(N_0'). \end{aligned}$$

従って, 全単射 $g : P \longrightarrow N_0$ が存在する.

$$f' : (N_0 + N_0') \times (N_0 + N_0') \longrightarrow N_0 + N_0'$$

を, $N_0 \times N_0$ 上 f_0 とし, P 上 g_0 と定める. すると, f' は全単射となり, $(N_0 + N_0', f') \in S$ となり, (N_0, f_0) の極大性に反する.

最期に, $\mathfrak{m} = \mathrm{card}(X) > \mathfrak{n} = \mathrm{card}(Y) > 0$ の場合を示す. このとき

$$\mathrm{card}(X \times X) \geq \mathrm{card}(X \times Y) \geq \mathrm{card}(X).$$

従って, Bernstein の定理により, $\mathfrak{m} = \mathrm{card}(X) = \mathrm{card}(X \times Y) = \mathfrak{mn}$. □

X を集合とし, $Y = \{0, 1\}$ とする. $Y = \{0, 1\}$ とするとき, X の任意の部分集合 A と, A の定義関数 χ_A とを同一視することにより, 次が成り立つ（命題 A.2.16）:

$$\mathcal{P}(X) = Y^X.$$

従って, $\mathfrak{m} = \mathrm{card}(X)$ とすれば, $\mathrm{card}(\mathcal{P}(X)) = 2^{\mathfrak{m}}$.

定理 A.6.21 $\mathfrak{m} > 0$ に対し, $2^{\mathfrak{m}} > \mathfrak{m}$.

証明 写像 $\mathfrak{m} = \mathrm{card}(X)$ とし, X の冪集合を $\mathcal{P}(X)$ とする.

$$X \longrightarrow \mathcal{P}(X), \quad x \longmapsto \{x\}$$

は単射なので, $\mathrm{card}(X) \leq \mathrm{card}(\mathcal{P}(X))$. ここで, 等号が成り立たないことを示す. もし, $\mathrm{card}(X) = \mathrm{card}(\mathcal{P}(X))$ ならば, 全単射

$$f : X \longrightarrow \mathcal{P}(X)$$

が存在する. さて

$$Y = \{x \in X \mid x \notin f(x)\}$$

とすると, f は全単射なので, $f(y) = Y$ となる, $y \in X$ が存在する. $y \in Y$ ならば, $y \in f(y) = Y$. 一方 Y の定義より, これは, $y \notin f(y) = Y$ となり, 不合理である. また, $y \notin Y = f(y)$ ならば, Y の定義より, $y \in Y$. これもまた不合理である. いずれにしても不合理である. よって, $\mathfrak{m} = \mathrm{card}(X) = \mathrm{card}(\mathcal{P}) = 2^{\mathfrak{m}}$ では有り得ない. □

系 A.6.22 *$\mathfrak{m} \geq \aleph_0$, $\mathfrak{m} \geq \mathfrak{n} \geq 2$ ならば, $\mathfrak{n}^{\mathfrak{m}} = 2^{\mathfrak{m}}$.*

証明 前定理より, $2^{\mathfrak{n}} \geq \mathfrak{n}$. 従って,

$$(2^{\mathfrak{n}})^{\mathfrak{m}} \geq \mathfrak{n}^{\mathfrak{m}}.$$

ここで, 命題 **??** より,

$$(2^Y)^X = \mathrm{Map}(X, \mathrm{Map}(Y, \{0,1\}) \simeq \mathrm{Map}(X \times Y, \{0,1\}) = 2^{X \times Y}.$$

定理より, $\mathrm{card}(2^{X \times Y}) = \mathrm{card}(2^X)$ を得る. よって, $\mathrm{card}(2^X) \geq \mathrm{card}(Y^X)$. 一方, $\mathrm{card}(Y^X) \geq \mathrm{card}(2^X)$ は明らかであり, Bernstein の定理より, 結論を得る. □

例 A.6.2 *$I = \{0, 1, 2, \cdot, 9\}$ とすると*

$$f : I^{\mathbb{N}} \longrightarrow [0,1); \qquad (a_n)_{n \in \mathbb{N}} \longrightarrow 0.a_1 a_2 \cdots a_n \cdots \quad (a_n = f(n))$$

は全射である. 定理 **??** *(1)* により, $\mathrm{card}([0,1)) \leq \mathrm{card}(I^{\mathbb{N}})$. また,

$$\{1,2\}^{\mathbb{N}} \longrightarrow [0,1); \quad (b_n)_{n \in \mathbb{N}} \longmapsto 0.b_1 b_2 \cdots b_n \cdots \quad (b_n = f(n) \in \{1,2\})$$

は単射である. 従って $\mathrm{card}(\{1,2\}^{\mathbb{N}}) \leq \mathrm{card}([0,1))$. $\mathrm{card}(2^{\mathbb{N}}) = \mathrm{card}(I^{\mathbb{N}})$ なので, $\mathrm{card}([0,1)) = \mathrm{card}(2^{\mathbb{N}})$. 一方, $(0,1) \subset [0,1) \subset \mathbb{R}$ であり, $(0,1) \simeq \mathbb{R}$ なので,

$$\mathfrak{c} = 2^{\aleph_0}).$$

また, $\mathfrak{f} := \mathrm{card}(2^{\mathbb{R}}) = 2^{\mathfrak{c}}$ とすると, 定理により, $2^{\mathfrak{c}} = \mathfrak{c}^{\mathfrak{c}}$ となるので

$$\mathfrak{f} = \mathrm{card}(\mathrm{Map}(\mathbb{R}, \mathbb{R})).$$